BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 10-245

30 MARCH 2009

DOVER AIR FORCE BASE Supplement

8 AUGUST 2012

Operations

ANTITERRORISM (AT)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **http://www.e-publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AF/A7S

Certified by: HQ USAF/A7S (Brig Gen Mary Kay Hertog)

Supersedes: AFI10-245, 21 June 2002

Pages: 117

(DOVERAFB)

OPR: 436 AW/AT

Certified by: 436 AW/AT (Mr. Michael Mendoza)

Supersedes: AFI10-245_AMCSUP_ DOVERAFBSUP, 1 December 2005

Pages:48

This instruction implements AFPD 10-2, *Readiness*; Department of Defense Directive (DODD) 2000.12, *Antiterrorism (AT) Program*; Department of Defense Instruction (DODI) 2000.16, *Antiterrorism (AT) Standards*. It establishes responsibilities and guidance for the Air Force (AF) Antiterrorism (AT) Program and integrates security precautions and defensive measures. This Air Force Instruction (AFI) applies to all military and civilian Air Force personnel, Air Force Reserve Command and Air National Guard units and other individuals or organizations as required by binding agreement or obligation with the Department of the Air Force. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at **https://www.my.af.mil/gcss-af61a/afrims/afrims/rims.cfm**. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF IMT 847, *Recommendation for Change of Publication*; route AF IMT 847s from the field through the appropriate functional's chain of command.

(DOVERAFB) AFI 10-245, 30 Mar 2009 is supplemented as follows: This supplement applies to all personnel assigned to or attached to the 436th Airlift Wing and tenant organization operating on Dover AFB to include the 512th Airlift Wing (AFRC). This supplement establishes 436th Airlift Wing guidance and policies that cover Antiterrorism (AT) Standards. It is designed to be used in conjunction with AFI 10-245, *Air Force Antiterrorism (AT) Standards* and AMC Supplement 1 to AFI 10-245. This supplement fulfills the necessary requirements to implement an Installation level Antiterrorism program.

SUMMARY OF CHANGES

This document is substantially revised and must be completely reviewed. It incorporates revisions to DODD 2000.12 and DODI 2000.16 including the requirement for an AT level II certified Antiterrorism Officer; the applicability of AT Standards to non-DoD tenants on DoD property; and updated DoD AT Standards. AF functional roles and responsibilities were added or updated to align with the A-staff construct; and several FPCON measures have been revised or updated, to include measures addressing Biological Select Agents and Toxins (BSAT) and Chemical, Biological, Radiological and Nuclear CBRN). Attachment 2-- References to DOD O-2000.12-H, Attachment 4-- AOR-Specific Training, and Attachment 8-- Antiterrorism Resource Allocation Template were removed and replaced with Attachment 4-- Risk Management and Resourcing processes. The following Report Control Symbol (RCS) requirements were removed: HAF-SFC(AR)0126, Training Reports for Antiterrorism Level I and Level II Training, and HAF-SFC(SA)0125, Status of Antiterrorism Report.

(DOVERAFB) This document is substantially revised and must be completely reviewed. Some of the most notable changes are: Combines the AT Working Group (ATWG) and the Critical Asset Risk Management (CARM) Program Working Group into the Force Protection Working Group (FPWG). Designates the CARM Manager as a core member on the local Terrorist Vulnerability Assessment Team. Includes the Hotel Assessment Security Checklists as an attachment and appoints the FSS as the Installation lead for these assessments. Establishes a formal annual Unit AT Program Review guide and grading criteria. Specifies local suspicious activity reporting procedures IAW DoD's 14 reportable categories. Designates the 436 SFS/S2 (Force Protection Intelligence) as the Installations Threat/Intelligence Fusion Cell (TIFC) and outlines their roles/responsibilities. Requires the Wing Commander be out-briefed on all functional Vulnerability Assessment (VA) results for validation and approval prior to release to higher headquarters via Core Vulnerability Assessment Management Program (CVAMP).

Chapter 1

AIR FORCE ANTITERRORISM PROGRAM

1.1. Air Force Antiterrorism Program. This instruction establishes guidance and procedures for the Air Force (AF) Antiterrorism (AT) Program supporting the Department of Defense (DOD) AT Program. The program seeks to deter or limit the effects of terrorist acts against the AF by giving guidance on collecting and disseminating timely threat information, providing training to all AF members, developing comprehensive plans to deter and counter terrorist incidents, allocating funds and personnel and implementing AT measures.

1.1. (DOVERAFB)DAFB AT Program. The Dover AFB Antiterrorism (AT) program enhances and supplements current DoD, AF and AMC AT programs. The Installation AT program provides a comprehensive and structured means to identify antiterrorism measures and procedures for the protection of all personnel and property assigned to Dover AFB. This program does not cover each and every contingency with regard to Antiterrorism, Weapons of Mass Destruction, Mass Casualty, or Emergency Response. The DAFB AT program provides guidance to implement antiterrorism measures, mitigate vulnerabilities, and provide emergency response to terrorist incidents or situations occurring on Dover AFB. This program, compliments other Wing plans, addressing contingency and emergency response.

1.1.1. AT Responsibility. AT is a command responsibility and must be thoroughly integrated into every unit mission. Commanders must continually review their AT posture to keep current with changing policies and threat levels. Risk management is the key when determining vulnerabilities and resource prioritization. Any threat or potential vulnerability with risk that cannot be controlled to an acceptable level must be forwarded to the next level in the chain of command for resolution. AT also requires every individual's participation to maintain awareness, practice personal security measures and report suspicious activity.

1.1.1. **(DOVERAFB) DAFB AT Responsibility.** AT requires an integral effort of all Dover AFB units. All Dover AFB commanders (host, tenant, and temporarily assigned units) must have the mindset their unit is an integral part of the AT Program and Force Protection is a team effort, not the sole responsibility of the Security Forces unit. The driving purpose of the Dover AFB AT Program is to deter, defend, and strengthen the Installation against terrorist plans and operations in order to preserve the fighting strength of 436 AW and tenant forces to execute assigned wartime missions. The 436 AW Antiterrorism Officer (436 AW/AT) is the primary advisor for the Wing's Antiterrorism Program. The Installation Commander's Intent for AT is as follows:

1.1.1.1. **(Added-DOVERAFB)** Dover AFB has a three tier AT Corporate Structure consisting of the following levels: (1) Force Protection Executive Council (FPEC), (2) Force Protection Working Group (FPWG), and the (3) Threat Working Group (TWG).

1.1.1.2. **(Added-DOVERAFB)** DAFB can mitigate and reduce the vulnerability to terrorist actions by; developing and utilizing available intelligence/counterintelligence assets, maintaining established standards, training all Installation personnel, and by encouraging AT awareness within the community. DAFB will institute a progressive system of protective measures, policies and plans that display an effective AT position,

with the overall intent being the protection of all Installation personnel, families, assets, critical infrastructure, and mission effectiveness from any acts of terrorism.

1.1.2. Countering the Threat. Countering the terrorist threat requires a fully integrated and coordinated AT approach with a number of key areas that include at a minimum: Civil Engineers (Readiness and Emergency Management, Facilities Engineering, Explosive Ordnance Disposal (EOD) and Fire Emergency Services), chemical, biological, radiological, nuclear and high-yield explosives (CBRNE) defense, Services (food), Public Affairs, Communications, Intelligence, Operations, Security Forces, Surgeon General, Judge Advocate, Comptroller and Air Force Office of Special Investigations (AFOSI). AT programs should be coordinated with overarching efforts to achieve protection, such as Force Protection (FP), critical infrastructure protection and continuity of operations, as described in Joint Publication (JP) 3-07.2, *Antiterrorism*.

1.1.2. **(DOVERAFB)** Coordination among various components of Antiterrorism is critical. At a minimum, the following major plans or programs shall be synchronized to allow for broad spectrum protection:

1.1.2.1. **(Added-DOVERAFB)** Integrated Defense Plan (IDP). OPR: SFS.

1.1.2.2. **(Added-DOVERAFB)** Critical Infrastructure Protection (CIP). OPR: AT.

1.1.2.3. **(Added-DOVERAFB)** Medical Contingency Response Plan (MCRP) and Disease Containment Plan (DCP). OPR: MDG.

1.1.2.4. **(Added-DOVERAFB)** Emergency Management (EM) and Contingency Response Planning. OPR: CES.

1.1.3. DOD Policy. DODD 2000.12, *DOD Antiterrorism (AT) Program*, establishes the DOD policies and responsibilities for the implementation of the DOD AT Program. It establishes DODI 2000.16, *DOD Antiterrorism (AT) Standards*, and DOD O-2000.12-H, *Antiterrorism Handbook*. The DOD AT Program is a sub-element of Combating Terrorism (CbT). Combating Terrorism is a pillar of FP.

1.1.3.1. An active AT program utilizes DOD AT Standards prescribed in DODI 2000.16 as baseline standards. AF AT Standards in Chapter 2 of this document incorporate and supplement the DoD AT Standards and provide AF specific guidance.

1.1.3.1.1. Geographic Combatant Commander AT policy precedence. In accordance with the Unified Command Plan (UCP) and DODD 2000.12, the Geographic Combatant Commander (GCC) AT policies take precedence over the AT policies and programs of any other DOD Component operating or existing in the GCC area of responsibility (AOR) except for those under the security responsibility of a Chief of Mission (CoM), to include exercising tactical control (TACON) for FP. TACON for FP is in addition to a Combatant Commander's normal exercise of operation control (OPCON) over assigned forces. All DOD personnel traveling into a GCC's AOR shall familiarize themselves and comply with all AOR-specific AT policies. AF Components to GCCs bridge gaps between GCC and AF policies. In the application of AT policy the more restrictive guidance will be applied.

1.1.4. Non-DOD Tenants on AF Property. Commanders shall ensure that there is a host tenant agreement with all non-DOD tenants on AF property and that it specifically obligates

the non-DOD tenant to comply with the AT requirements in this AFI. Non-DOD tenants on an AF installation, facility or other AF property will be incorporated into, comply with and support installation security and AT Program requirements. Non-DOD tenants on AF property must comply with all aspects of the AT Program addressed in this Instruction and other AT guidance documents unless the facility is outside of the installation controlled perimeter; DOD personnel occupy less than 25% of the facility's net interior useable area in accordance with Unified Facilities Criteria (UFC) 4-010-01, *DOD Minimum Antiterrorism Standards for Buildings*; and the installation commander determines AT compliance is not required for that facility.

1.1.4. **(DOVERAFB)** The 436AW will ensure provisions for AT compliance are included in all host-tenant agreements.

1.1.5. Overseas Travel. All AF military personnel, civilians, dependent family members and contractors when supporting DOD operations in accordance with contract provisions and outside of the United States shall comply with theater, country and special clearance requirements (AFI 24-405, *Department of Defense Foreign Clearance Guide*, and DOD 4500.54-M, *DOD Foreign Clearance Manual*) before traveling outside the continental United States (OCONUS).

1.1.6. Eagle Eyes. The Eagle Eyes program is an Air Force AT defensive program created to enhance the collection of threat information by educating members of the Total Force and off-base citizens on the nature of terrorist attack-planning activities. Eagle Eyes is a command responsibility and requires every individual's participation to maintain awareness, practice personal security measures and report suspicious behavior. Every AF installation will establish procedures to receive reports of suspicious behavior or indications of terrorist activity.

1.1.6. **(DOVERAFB)** Det 306, AFOSI is the OPR for the Installation Eagle Eyes Program. All personnel are encouraged to report suspicious activity to the servicing Security Forces or AFOSI Detachment. Eagle Eyes reports will be identified and annotated in the Security Forces blotter and appropriate agencies notified for investigation and follow-up.

1.1.6.1. **(Added-DOVERAFB)** Suspicious activity reporting will be conducted in accordance with instructions contained in 436 AW OPLAN to 10-245.

1.1.6.1.1. **(Added-DOVERAFB)** Det 306, AFOSI and Security Forces are the lead investigative agencies for suspicious activity reporting.

1.1.6.1.2. **(Added-DOVERAFB)** The 436 SFS/S2 (Force Protection Intelligence) is designated as the Installation Threat/Intelligence Fusion Cell (TIFC) and monitors, tracks and disseminates all suspicious activity reporting to the Core Threat Working Group.

1.2. Roles and Responsibilities.

1.2.1. General. AF commanders or civilian equivalent directors assigned AT responsibility shall establish active AT programs using DOD AT Standards prescribed in DODI 2000.16 as baseline standards to reduce vulnerability to terrorism. AF unique requirements contained in this Instruction supplement DOD AT Standards.

1.2.1.1. Major commands (MAJCOMs), field operating agencies (FOAs), direct reporting units (DRUs), AF Components to the GCC, component-numbered AFs (C-NAFs), numbered AFs (NAFs), wings, installation and self-supported separate facilities and commanders or civilian equivalent directors assigned AT responsibility shall have an AT program tailored to the local mission, conditions, terrorist threat and national security environment.

1.2.1.2. Supplements to this instruction by AF activities, such as MAJCOM or installation supplements, shall identify AT specific operational responsibilities. Responsibilities shall include the scope of AT programs for facilities and operations that do not meet the legal definition of an installation, e.g. recruiting offices, Rapid Engineer Deployable Heavy Operations Repair Squadron (RED HORSE) at Guam and other geographic separated units (GSUs).

1.2.1.3. AF activities and action to combat terrorism shall support the GCC as they exercise overall responsibility for AT within their respective AOR. Ensure such activities and actions comply with applicable status of forces agreements (SOFA) and the *DOD Foreign Clearance Manual*.

1.2.1.4. All commanders have the authority and responsibility to enforce appropriate security measures to ensure the protection of DOD elements and personnel subject to their control while pursuing mission accomplishment and shall ensure the AT awareness and readiness of all DOD elements and personnel assigned or attached.

1.2.1.4.1. **(Added-DOVERAFB)** Commanders may use the Installation Force Protection Executive Council as a forum to initiate discussion on any AT awareness or readiness concerns.

1.2.1.4.2. **(Added-DOVERAFB)** Group, squadron, tenant commanders, and staff agency chiefs will:

1.2.1.4.2.1. **(Added-DOVERAFB)** Ensure their unit/agency is in compliance with all AT measures and staff directives. NOTE: When a facility is occupied by more than one unit, the senior commander is responsible for ensuring the facility as a whole is in compliance of AT standards.

1.2.1.4.2.2. **(Added-DOVERAFB)** Publish a Unit Antiterrorism Operating Instruction (OI) for areas under their control. Unit OIs will address: development and maintenance of a continuity binder, selection and turnover procedures for appointed representatives, Random Antiterrorism Measures (RAMs), Unit AT awareness and training program, Wing and Unit specific implementation of Force Protection Conditions (FPCONs), Self-Inspection requirements and procedures, building evacuation plans for both fire and bomb threats, and describe the duties and responsibilities of the unit's AT Representative. Units with contingency response plan requirements (e.g., Security Forces, Medical, Civil Engineer) may incorporate them into existing plans as long as all elements are addressed.

1.2.1.4.2.3. **(Added-DOVERAFB)** Include AT awareness at Commander's Calls periodically throughout the year.

1.2.1.4.2.4. **(Added-DOVERAFB)** Encourage family members of assigned

personnel to obtain Level I AT Awareness training annually.

1.2.1.4.2.5. **(Added-DOVERAFB)** Ensure all DoD personnel under their command requesting non-official personal travel oversees to high-threat or restricted countries must complete an Individual Antiterrorism Travel Plan (refer to USNORTHCOM and State Dept Travel Advisories). In addition, the member will receive required threat/intelligence briefs, completed supplemental AT/FP training and obtain applicable commander level approval prior to OCONUS travel IAW Higher Headquarters directives.

1.2.1.5. For more effective host nation (HN) support commanders shall, as appropriate:

1.2.1.5.1. Ensure HN and/or civil support agreements for AT mutual support are established and exercised with HN/civil support.

1.2.1.5.2. If required HN/civil support agreements to support AT are not established and implemented, up-channel notification of the situation to MAJCOMs and/or AF Components to GCCs, who shall determine if the GCC has agreements established. If not, document the shortfall and inform the AF/A7S.

1.2.1.5.3. Ensure procedures for information sharing are established and implemented within the commander's span of control in accordance with GCC or CoM guidance or agreements (SOFA, Mutual Aid Agreement (MAA), etc.) and ensure appropriate personnel under their authority, who are responsible for supporting the classification and declassification of records, receive appropriate training.

1.2.1.5.4. Adopt the following key elements to enhance HN support and ensure this information is in AT policy and training: HN support agreements, resources and benefits provided by the United States, working groups and informal outreach activities, training and exercises with HN officials, threat information sharing and positive human capital attributes of key AF personnel, such as right skills, training and duty tour length.

1.2.1.5.5. For OCONUS permanent or expeditionary assignments, identify qualified interpreters or provide language and cultural training for those personnel filling key positions interacting with HN personnel; consider improving cultural training for all OCONUS permanent party and for pre-deployment.

1.2.2. Financial Management (FM). The FM shall:

1.2.2.1. Advise commanders, the AT Working Group (ATWG) and AT Executive Committee (ATEC) on financial processes and procedures to effectively resource AT program requirements through the planning, programming, budgeting and execution (PPB&E) and Combating Terrorism Readiness Initiative Fund (CbT-RIF) processes in conjunction with other staff offices.

1.2.2.2. Provide long range financial planning for the AT Program.

1.2.3. Inspector General (IG). The Inspector General will evaluate the commander's ability to execute an AT program and the overall AT program effectiveness will be recorded in accordance with AFI 90-201, *Inspector General Activities*.

1.2.4. Judge Advocate (JA). The JA will provide legal advice on AT matters.

1.2.5. Public Affairs (PA). The PA shall:

1.2.5.1. Incorporate communication activities to combat terrorism in the public affairs program.

1.2.5.2. Coordinate all terrorist incident/threat report releases to the media with the commander's Threat Working Group (TWG) prior to the unit commander's approval for release.

1.2.5.3. In response to a possible or real terrorist threat, the PA representative, after coordination with the commander's TWG and the Office of the Assistant Secretary of Defense (OASD)/PA, may acknowledge that increased security measures have been taken. Requests for coverage of counter-terrorism forces will not be approved.

1.2.5.4. **(Added-DOVERAFB)** 436 AW/PA will support the antiterrorism program through appointed membership in the Threat and Force Protection Working Groups, support to Force Protection Condition (FPCON) actions/measures, and direct liaison with the 436 AW/ATO for periodic AT awareness initiatives.

1.2.5.5. **(Added-DOVERAFB)** 436 AW/PA will coordinate all terrorist incident/threat report releases to the media with the Installation's Threat Working Group (TWG) prior to the Wing Commander's approval for release.

1.2.5.6. **(Added-DOVERAFB)** In response to a possible or real terrorist threat, the PA representative, after coordination with the Installation's TWG and the Office of the Assistant Secretary of Defense (OASD)/PA, may acknowledge that increased security measures have been taken. Requests for coverage of counter-terrorism forces will not be approved.

1.2.5.7. **(Added-DOVERAFB)** 436 AW/PA will prepare pre-approved canned press releases for individual AT Threat Planning scenarios outlined in Table 2.1 of AFI 10-245.

1.2.6. Surgeon General (SG). The SG shall:

1.2.6. **(DOVERAFB)** 436 MDG will support the antiterrorism program through appointed membership in the TWG and Force Protection Working Group (FPWG).

1.2.6.1. Serve as the OPR for Force Health Protection (FHP) and the Public Health Emergency Officer (PHEO) in accordance with AFI 10-2603, *Emergency Health Powers on Air Force Installations*.

1.2.6.2. Participate in the food and water protection programs as outlined in AFI 10-246, *Food and Water Protection Program*.

1.2.6.3. Ensure food and water vulnerabilities and toxic industrial chemical/toxic industrial material (TIC/TIM) vulnerabilities related to terrorism are entered in the Core Vulnerability Assessment Management Program (CVAMP), through the Antiterrorism Officer (ATO), and are tracked to the commander's risk acceptance or resolution.

1.2.6.3. **(DOVERAFB)** 436 MDG will utilize DoD standards to identify observations (vulnerabilities or concerns) for inclusion into CVAMP. Track/monitor all open observations until closed or carried over into a new Vulnerability Assessment (VA) report. The Wing Commander will be out briefed on the VA results for validation and approval to release in to HHQ using CVAMP.

1.2.7. Safety (SE). SE shall assist functional areas in ensuring safety is observed during AT operations and incident management contingencies.

1.2.8. Manpower, Personnel and Services (A1). The A1 shall:

1.2.8.1. Provide AT policy and guidance for personnel issues.

1.2.8.2. Provide specific policy and guidance for documenting pre-deployment AT training and special position or duty qualifications on deployment orders.

1.2.8.3. Ensure a system exists for tracking formal AT training (Standard 24).

1.2.8.4. Serve as the OPR for incorporating and utilizing AT processes concerning food handling and distribution.

1.2.8.5. Assist in the review of Capability Based Manpower Standards and manpower determinant tools for appointed AT positions, e.g. ATOs, as described in AFI 38-201, *Determining Manpower Requirements*.

1.2.8.6. Notify AF/A7S when a deficiency is identified in manpower standards supporting appointed AT positions.

1.2.9. Intelligence, Surveillance and Reconnaissance (A2). The A2 shall provide Intelligence support as directed in AFI 14-119, *Intelligence Support to Force Protection*.

1.2.9. **(DOVERAFB) 436 OG/OGI** will support the antiterrorism/force protection program through appointed membership in the TWG and FPWG.

1.2.10. Operations (A3). The A3 shall:

1.2.10.1. Identify AT requirements and desired effects for mission operations.

1.2.10.2. Ensure operational reporting procedures for AT associated events are established and exercised.

1.2.10.3. AF/A3/5 is the OPR for Air Force AT matters and policies and approves all AF-wide AT programs.

1.2.10.4. **(Added-DOVERAFB) Wing Plans and Programs (XPO).** Wing Plans will ensure AT is factored into operational plans, exercise plans, and other antiterrorism/force protection contingency plans, affecting the security of Installation personnel and operational resources.

1.2.11. Logistics Readiness (A4). The A4 shall:

1.2.11.1. Provide Supply Chain Management to fulfill AT requirements.

1.2.11.2. Monitor logistics readiness AT program support.

1.2.11.3. Manage Airmen support requirements (protective equipment, weapons, etc).

1.2.11.4. Incorporate AT considerations in the expeditionary support planning program.

1.2.12. Operational Plans and Requirements (A5). The A5 shall ensure AT is factored into operational plans, pre-deployment site surveys, airfield, work center, billets and recreation site selections.

1.2.13. Communication (A6 or XC). The A6 or XC shall:

1.2.13. **(DOVERAFB) 436 Communications (CS).** CS will support the antiterrorism program through liaison with the TWG and appointed membership in the FPWG.

1.2.13.1. Ensure net-centric communications and information (C&I), to include wireless, radio and satellite communications, identifies and links Information Operations capabilities that support AT and provides routine AT communications management and command and control.

1.2.13.2. Assist in the identification of C&I requirements for the AT Program and provide technical solution and rough order of magnitude costings.

1.2.13.3. Ensure C&I vulnerabilities in information systems that support AT Programs are entered into CVAMP, through the ATO, and documented in the system security certification and accreditation package. The vulnerability should be documented as a plan of action and milestone (POA&M) as defined in AFI 33-202, vol 1 *Network and Computer Security*.

1.2.13.4. Provide AT policy and guidance for mail handling and management.

1.2.14. Installation and Mission Support (A7). The A7 shall:

1.2.14. **(DOVERAFB)** 436 CES will support the antiterrorism program through appointed membership in the TWG and FPWG. CES will ensure the Comprehensive Emergency Management Plan (CEMP 10-2) is fully coordinated and synchronized with the Wing AT Plan.

1.2.14.1. Ensure installation capabilities and resources support the AT Program and are incorporated in appropriate aspects of air, space and information operations, plans and requirements.

1.2.14.2. Ensure appropriate capabilities of the AT Program are integrated with the Emergency Management (EM) Program as defined in AF Policy Directive (AFPD) 10-25, *Emergency Management*, and AFI 10-2501, *Air Force Emergency Management (EM) Program, Planning and Operations*.

1.2.14.3. Implement terrorism incident planning for response, consequence management and recovery within AT Programs.

1.2.14.4. Provide engineering infrastructure protection expertise to counter terrorist threats.

1.2.14.5. Ensure installation programmers and engineers are trained in FP and AT and incorporating the latest DOD and UFC standards in all designs.

1.2.14.6. Contracting officers, in coordination with program managers and requirement officials, ensure AT clauses required by Defense Federal Acquisition Regulation (DFAR) and supplements and local AT measures provided as part of the requirement are incorporated into AF contracts (Standard 18).

1.2.14.6. **(DOVERAFB)** 436 CONS will support the antiterrorism program through appointed membership in the FPWG and assist the Wing ATO in developing local contract considerations as well as coordination of AT-specific mitigation projects.

1.2.14.7. Provide physical security and provost service capabilities to support AT.

1.2.14.8. Ensure appropriate capabilities of the AT Program are integrated with Integrated Defense as defined in AFPD 31-1, *Integrated Defense.*

1.2.14.8.1. **(Added-DOVERAFB)** 436 SFS/CC will support the antiterrorism program through appointed membership in the TWG and FPWG. Ensure Integrated Defense (ID) plans are fully coordinated and synchronized with the Wing AT program. Establish an Installation Threat/Intelligence Fusion Cell (TIFC).

1.2.14.8.2. **(Added-DOVERAFB) 436 SFS Force Protection Intelligence (S2).** The S2 will serve as the Installation Threat/Intelligence Fusion Cell (TIFC) and work under the direction of the Installation TWG Chair.

1.2.14.8.3. **(Added-DOVERAFB)** The 436 SFS/S2 in conjunction with other information production agencies shall produce substantive Antiterrorism/Force Protection intelligence summaries, threat and informational products for the AW/ATO, TWG, FPWG, operations planners and Wing senior leadership (AW/CC, AW/CV and Group Commander). Review all-source intelligence effecting local security postures and recommend courses of action to the TWG and AW/ATO.

1.2.14.9. Ensure engineering infrastructure, installation and/or facility design, physical security, resource protection, fire emergency services, EOD, expeditionary engineering, and readiness and emergency management vulnerabilities related to terrorism are entered in CVAMP, through the ATO, and the Automated Civil Engineering System (ACES).

1.2.14.10. AF/A7S drafts and coordinates AF-wide AT matters, policies and programs.

1.2.15. Strategic Plans and Programs (A8). The A8 shall:

1.2.15.1. Provide long-term planning and programming for AT programs and processes.

1.2.15.2. Develop, integrate and analyze AT initiatives for AF Future Years Defense Program (FYDP) and long range plan to support the National Military Strategy for Combating Terrorism.

1.2.15.3. Ensure AT programming initiatives are considered for operational impact during PPB&E processes.

1.2.16. Air Force Office of Special Investigations (AFOSI). Provides the Air Force a capability to conduct Counterthreat Operations (CTO) to detect and assess – *find, fix, track and neutralize* the enemy threat as described in AF Tactics, Techniques, and Procedures (AFTTP) 3-10.3, *Integrated Defense Counterthreat Operations (CTO).* AFOSI is the lead Air Force agency for collection, investigation, analysis and response for threats arising from terrorists, criminal activity and foreign intelligence and security services as described in AFPD 71-1, *Criminal Investigations and Counterintelligence* and AFI 14-119, *Intelligence Support to Force Protection (FP).*

1.2.16.1. Provides personal protective services for High-Risk Personnel (HRP) based on threats and in accordance with DODI O-2000.22, *Designation and Physical Protection of DOD High Risk Personnel* and AFI 71-101, vol 2, *Protective Service Matters.*

1.2.16.1. **(DOVERAFB)** Det 306, AFOSI will support the antiterrorism program through appointed membership in the TWG, FPWG and Vulnerability Assessment Teams.

1.2.17. Antiterrorism Officers (ATOs). The ATO is the commander's military or civilian advisor charged with managing the AT Program. Responsibilities are outlined in Standard 9.

1.2.18. Unit AT Representative. Unit AT representatives are appointed in writing for units and DOD elements and personnel not required to have an ATO as stipulated in Standard 9. Unit AT representatives are charged with managing the AT Program for their unit or DOD element and personnel. Responsibilities are further described in paragraph 2.9.5.

Chapter 2

ANTITERRORISM STANDARDS

2.1. Standard 1: AT Program Elements. The minimum required elements of an AT program shall be: risk management (Standard 3); planning (including development of the AT Plan) (Standard 7); training and exercises (Standard 23); resource application (Standard 30); and comprehensive program review (Standard 31). The development and maintenance of the AT Program elements should be ongoing and continuously refined to ensure the relevance and viability of all measures employed to reduce vulnerabilities to terrorist capabilities.

2.2. Standard 2: Intelligence Support to the AT Program.

2.2.1. The Defense Intelligence Agency (DIA) sets the DOD Terrorism Threat Level (TTL). This threat level identifies the potential threat to DOD interests in a particular country, including the United States. The DOD TTL applies whether or not U.S. personnel are present in the country. GCCs may also set terrorism threat levels for specific personnel, family members, units, installations or geographic regions in countries within the GCC AOR. See Attachment 3 for more information on TTLs.

2.2.2. Commanders of MAJCOMs, AF Components to the GCC, C-NAFs, NAFs, wings, installations or self-supported separate facilities or deployed commanders assigned AT responsibility shall:

2.2.2.1. Task the appropriate officials under their command or control to gather, analyze and circulate appropriate terrorism threat information. When local information indicates gaps, commanders shall forward timely requests for information via appropriate intelligence collection and production channels.

2.2.2.2. Identify Intelligence (A2) as the lead force protection intelligence (FPI) representative to develop Priority Intelligence Requirements (PIRs) for integration into the Commander's Critical Information Requirements (CCIRs) to focus collection and analysis efforts.

2.2.2.2. **(DOVERAFB)** 436 OG/OGI will assist AFOSI in developing Dover AFB Priority Intelligence Requirements (PIRs).

2.2.2.2.1. The AFOSI has the lead for continental United States (CONUS) related PIRs.

2.2.2.3. Provide units in transit with tailored terrorist threat information.

2.2.2.4. Integrate countersurveillance, surveillance detection, counterintelligence (CI) and other specialized skills into AT programs.

2.2.2.5. Identify an AFOSI official as the focal point for local or host-nation law enforcement intelligence, CI and criminal intelligence (CRIMINT) information.

2.2.2.5. **(DOVERAFB)** AFOSI Det 306/CC will appoint an agent in writing to 436 AW/AT to be the focal point for local or host-nation law enforcement intelligence, CI and criminal intelligence (CRIMINT) information. The appointed individual may be the same as the primary TWG representative.

2.2.2.6. Incorporate proactive techniques to detect and deter terrorists, particularly in support of assets or activities conducted in areas designated with SIGNIFICANT or HIGH TTLs. These activities shall include, but are not limited to: in-transit forces, HRP, special events and high-value military cargo shipments.

2.2.2.7. Ensure that subordinate commanders at all levels forward up and down the chain of command all information pertaining to suspected terrorist threats or acts of terrorism involving DOD elements and personnel or assets for which they have responsibility, including the provisions of such information to appropriate interagency officials.

2.2.2.8. Ensure subordinate commanders and key staff members are trained to maximize the use of information derived from law enforcement liaison from intelligence and CI processes and procedures. This includes intelligence procedures for handling PIR for in-transit units and the implementation of procedures to conduct intelligence preparation of the battle space and mission analysis.

2.2.3. Air Force intelligence, CI and law enforcement elements will coordinate the dissemination of information on U.S. persons to the Air Force as appropriate in support of the AT Program and within the provisions of AFPD 71-1, *Criminal Investigations and Counterintelligence*, AFI 71-101, Vol 1, *Criminal Investigations*, and DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons*.

2.3. Standard 3: AT Risk Management.

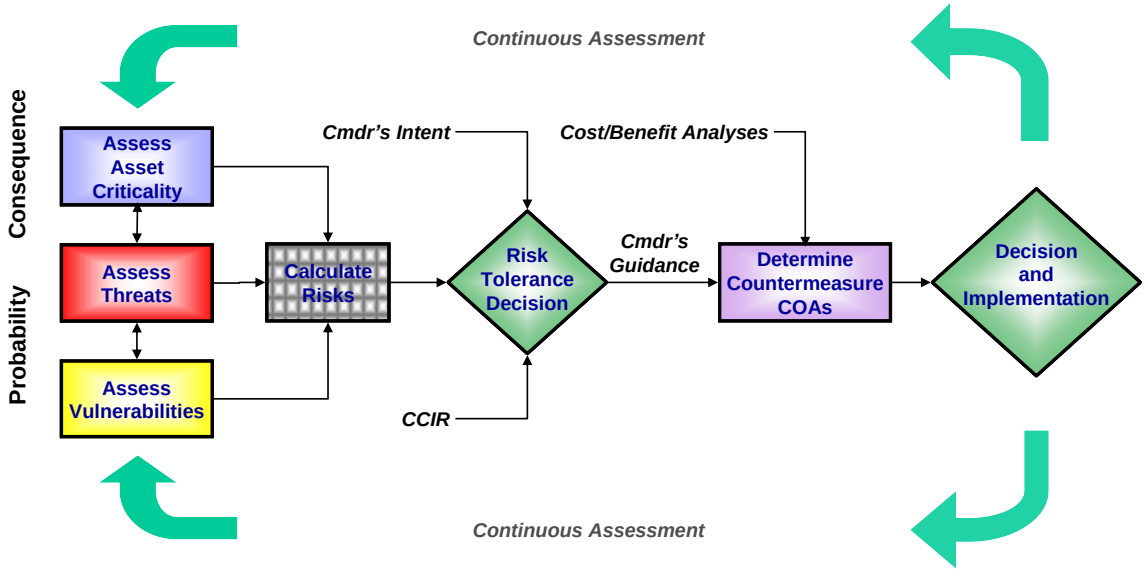
2.3.1. The AT risk management process is modeled upon the principles described in DOD O-2000.12-H and Integrated Defense Risk Management described in AFPD 31-1. It should be applied in all aspects of AT program implementation and planning, including operational plans and decisions, development of risk mitigation measures and the prioritization and allocation of resources. The essential components of AT risk management include: determining the criticality of assets (criticality assessment); assessing the terrorist threats (threat assessment); identifying the vulnerabilities of facilities, programs and systems to an attack, including the use of CBRNE or similar capabilities (vulnerability assessment); assessing risk based on a holistic understanding of the criticality, threat and vulnerability of the asset (risk assessment); and implementing the capabilities needed to correct or mitigate the risk (countermeasures) and reevaluating risk after countermeasures are employed; and/or accepting risk.

2.3.1.1. The AT risk management process and procedures shall be reviewed at least annually. An AT Program Review, a Higher Headquarters Assessment (HHA) or a Joint Staff Integrated Vulnerability Assessment (JSIVA) visit satisfies this requirement.

2.3.1.1. **(DOVERAFB)** The DAFB AT Risk Assessment (RA) process is contained within the Wing AT Plan 10-245 and is the cornerstone of AT Risk Management.

2.3.1.2. AT risk management is a continuous process of conducting operations. See Figure 2.1 for a graphical depiction.

Figure 2.1. AT Risk Management Process.



2.3.1.3. For deployments, AT risk management begins with the warning order.

2.4. Standard 4: Terrorism Threat Assessment.

2.4.1. Through the AFOSI and with support from the A2 and ATO a threat assessment process shall be established consistent with the principles outlined in DOD O-2000.12-H to identify the full range of known or estimated threat capabilities (including the use or threat of use of CBRNE). These assessments shall be updated on an annual basis or more frequently as the threat environment dictates or whenever the DIA or GCC TTL changes. Assessments shall be tailored to local conditions. For each group that may be a threat the assessment shall provide information on the group's intent, tactics, techniques and procedures (TTP), capability, probable course of action (COA) and history, as well as any specific targeting information that may be available. AFOSI is the AF agency responsible for preparing the DOD Threat Assessment (DTA) as prescribed in DODI 5240.18, *Counterintelligence Analysis and Production*.

2.4.1. **(DOVERAFB)** Upon completion of the annual AFOSI Threat Assessment (TA), the Installation TWG will include it in the Commander's Integrated Threat Assessment (CITA). The CITA will also include the Threat Matrix, Threat Scenarios, TIC/TIM Assessment, local Design Basis Threat (DBT), MANPAD Assessment, Criticality Assessment, and Mission Essential Venerable Areas (MEVAs). The CITA will be reviewed and updated by the Core TWG and approved by the Installation Commander annually.

2.4.2. Specific threat assessments are also prepared to support operational planning and risk decisions for unique mission requirements or special events including, but not limited to, in transit forces, training and exercises, and operational deployments.

2.4.3. Effective processes should be implemented to integrate and fuse all sources of available threat information from local, State, Federal and host-nation law enforcement agencies; the appropriate local, State, Federal and host-nation intelligence community activities; other local community officials and individuals; the applicable U.S. country team; port authority officials and husbanding contractors, as appropriate, to provide for a

continuous analysis of threat information to support the threat warning process in accordance with Standard 2.

2.4.4. Threat assessments are integrated into the AT risk management process as a major source of analysis and justification for recommendations and implementation of Random Antiterrorism Measures (RAMs); AT enhancements including physical security, emergency management or FHP changes; program and budget requests; and when conducting AT vulnerability assessments (VAs).

2.5. Standard 5: Criticality Assessment.

2.5.1. Criticality assessment processes shall be established consistent with the principles described in DOD O-2000.12-H and AFPD 31-1 to identify, classify and prioritize mission-essential personnel, assets and information. Criticality assessments shall also be conducted for non-mission essential assets such as high-occupancy buildings, mass gathering activities, energy infrastructure and any other facility, equipment, service or resource deemed important by the commander warranting protective measures to ensure continued efficient operation; protection from disruption, degradation or destruction; and timely restoration.

2.5.1.1. Criticality assessments should be coordinated with affected Defense Critical Infrastructure Program (DCIP) and Air Force Critical Infrastructure Programs (AF CIP), which follow the principles in DODD 3020.40, *Defense Critical Infrastructure Program (DCIP),* and AFPD 10-24, *Air Force Critical Infrastructure Program,* and identify defense critical infrastructure and critical assets.

2.5.1.1. **(DOVERAFB)** The 436 AW Critical Infrastructure Protection (CIP) Manager OPR is 436 AW/ATC. AF CIP is normally a separate program from AT. However, at Dover AFB the responsibility for the CIP program is assigned to the Installation AT office and appropriate full-time staff expertise will be resourced and assigned.

2.5.2. Criticality assessments will be updated at least annually to determine the degree of asset criticality based upon the following factors: relative importance, effect of loss, recoverability, mission functionality, substitutability and repairability. Criticality assessments shall provide the basis for identifying those assets that require specific protective measures and priorities for resource allocation when developing and updating AT-related contingency plans, e.g., AT Plan, Comprehensive Emergency Management Plan (CEMP) 10-2, Medical Contingency Response Plan (MCRP), Integrated Defense Plan (IDP), etc.

2.5.2. **(DOVERAFB)** The Installation AT Criticality Assessment will be reviewed annually by the FPWG and updated as needed.

2.6. Standard 6: Terrorism Vulnerability Assessment.

2.6.1. Vulnerability assessment processes shall be established consistent with the principles described in DOD O-2000.12-H and AFPD 31-1 to provide a vulnerability-based analysis of personnel (mission essential, mass gatherings, etc.) and mission essential assets (energy infrastructure, etc.) and information that are susceptible to terrorist threats. Incorporate food and water vulnerabilities according to the guidance in AFI 10-246. Incorporate other assessments, such assessments made through the DCIP and AF CIP, or coordinate schedules so teams visit the installation during the same time frame to reduce the impact on operational units.

2.6.1. **(DOVERAFB)** The local Terrorist VA will be led by the Wing ATO and conducted annually or as directed by the Installation Commander IAW DoDI 2000.16 and AFI 10-245. There are several other local functional areas or special purpose Force Protection related VAs required to be conducted annually by designated base SMEs. The following organizations are designed as the Installation lead agent for other local VAs:

Terrorism	OPR: 436 AW/AT (Antiterrorism)
Food Protection	OPR: 436 MDG (Public Health)
Water Protection	OPR: 436 MDG (Bioenvironmental)
TIC/TIM	OPR: 436 MDG (Bioenvironmental)
Critical Infrastructure	OPR: 436 AW/ATC (Critical Infrastructure)
All Hazards (aka CBRNE)	OPR: 436 CES/CEX (Emergency Management)

2.6.1.1. AF VA benchmarks provided by the AF Vulnerability Assessment Team (AFVAT), which include the JSIVA benchmarks, will be used. Within 90 days of a completed assessment, prioritize identified vulnerabilities, develop a plan of action to mitigate or eliminate the vulnerabilities and/or assume risk and report assessment results to the first general officer, flag officer or civilian equivalent director in the chain of command, to include the NAF.

2.6.1.2. CVAMP shall be populated with assessment results, vulnerabilities as a minimum, within 120 days from completion of the assessment, i.e. assessment outbrief.

2.6.1.2. **(DOVERAFB)** 436 AW/AT Office shall have SIPRNET connectivity established for access to CVAMP and classified threat and vulnerability assessment information.

2.6.1.3. A VA will be conducted at least annually or more frequently if the VA or mission requirements dictate. The VA will be conducted by a HHA team at least triennially. VAs shall be conducted at a minimum for, but not limited to:

2.6.1.3. **(DOVERAFB)** The Local Terrorism Vulnerability Assessment (LVA) process is contained within the AT Plan and will include all elements required by AMC supplement to AFI 10-245.

2.6.1.3.1. Any AF installation or AF owned or leased facility populated daily by 300 or more DOD personnel.

2.6.1.3.1. **(DOVERAFB)** HHQ and local VA reports will be managed by the designated/applicable OPR. All VAs will be out-briefed and validated by the Installation Commander. The FPWG will receive a comprehensive briefing on all open VA observations. The OPR will also coordinate with the Wing AT office to identify vulnerabilities and key observations requiring entry into CVAMP. All VA reports will be tracked and managed by the applicable OPR until all observations are closed; acceptance of risk by the Installation Commander or the observation is carried over into a new report.

2.6.1.3.2. Any AF installation or facility thereon bearing C2 responsibility for emergency response or physical security plans and programs, or determined to host

defense critical infrastructure or critical assets identified through the DCIP or AF CIP, or use, possess, transfer, or receive biological select agents and toxins (BSAT).

2.6.1.3.3. Any AF installation or AF owned or leased facility or activity possessing authority to interact with local non-military or host-nation agencies or having agreements with other agencies or host-nation agencies to procure these services.

2.6.1.3.4. AF hosted air ports of embarkation (POE) and debarkation (POD); movement routes (air, ground and rail); and assembly, staging, reception and final bed down locations in support of any battalion, squadron, ship, or equivalent operational deployment; and similar sized in-transit movement or training exercise. AF movement or shipment of military cargo shall be coordinated with the designated senior DOD Component with AT responsibility.

2.6.1.3.5. Any AF personnel designated as HRP (Standard 16). These assessments are referred to as Personal Security Vulnerability Assessments (PSVAs). PSVAs will conform to the formats of servicing Protection Providing Organizations (PPO) as identified in DODI O-2000.22. AFOSI is a designated PPO.

2.6.1.3.6. Any AF event or activity determined to be a special event or activity involving a gathering of 300 or more DOD personnel.

2.6.1.3.6. **(DOVERAFB)** Unit or Wing Project Officer planning or coordinating any event involving a gathering of 300 people or more will notify 436 AW/AT at least 90 days in advance of the expected event for Special Event Assessment (SEA) planning. The Dover SEA Planning Template contained within the AT Plan (APPENDIX 4 TO ANNEX B TO 436 AW AT PLAN 10-245), will be used to conduct assessments.

2.6.1.3.7. AF owned or leased off-installation housing, schools, daycare centers, commissaries, transportation systems and routes used by DOD personnel and their dependent family members when the TTL is SIGNIFICANT or higher, consistent with Standard 3. At locations where there are multiple DOD components or locations that are not AF owned or leased, VA requirements shall be coordinated with the designated senior DOD Component with AT responsibility.

2.6.1.4. Information derived from AT VAs shall be classified pursuant to the requirements outlined in the *Defense Threat Reduction Agency (DTRA)Joint Staff Integrated Vulnerability (JSIVA) Security Classification Guide*.

2.6.2. MAJCOMs and AF Components to the GCC will support the GCCs in scheduling assessments and prescribing policies for no-notice or short-notice movements to locations where a VA has not been accomplished or is not current. MAJCOMs should receive copies of reports on all VAs completed based on Standard 6.

2.7. Standard 7: AT Plan.

2.7.1. Commanders will develop and maintain a comprehensive AT plan for all DOD elements and personnel that the AF has AT responsibility. Use of the Joint Antiterrorism (JAT) Guide, when used in its entirety, satisfies all minimum planning elements prescribed in this instruction. These AT plans will not be considered complete unless signed by the commander and exercised. If applicable, synchronize the AT Plan with any existing CEMP and IDP. At a minimum, AT plans shall be developed at the installation and separate or

leased facility or space levels and for AF operational deployments, training exercises or events, and special events.

2.7.2. AT principles are incorporated into all operational plans and risk decisions using the standards prescribed by this instruction as a baseline to develop and implement AT policies in support of the AF's unique roles and mission requirements. Table 2.1. incorporates the Homeland Security Presidential Directive (HSPD) 8, *National Preparedness*. The OPR will recommend the appropriate planning parameters regarding the scale for AF operations and civil support operations based on the threat. Where A7C (CE) is designated the OPR, refer to AFI 10-2501.

Table 2.1. AT Threat Planning Scenarios.

Scenario	**Title**	**OPR**
1	Nuclear Detonation – 10-Kiloton Improvised Nuclear Device	A7C (CE)
2	Biological Attack – Aerosol Anthrax	A7C (CE)
4	Biological Attack – Plague	A7C (CE)
5	Chemical Attack – Blister Agent	A7C (CE)
6	Chemical Attack – Toxic Industrial Chemicals	A7C (CE)
7	Chemical Attack – Nerve Agent	A7C (CE)
8	Chemical Attack – Chlorine Tank Explosion	A7C (CE)
11	Radiological Attack – Radiological Dispersal Devices	A7C (CE)
12	Explosive Attack – Bombing Using Improvised Explosive Devices	A7C (CE)
13	Biological Attack – Food Contamination	SG3 (Medical)
15	Cyber Attack	XC or A6
16 (AF)	Armed Attack – Small Arms: Individual to Squad (10 pax)	A7S (SF)
17 (AF)	Aircraft Attacks in the Take-off and Landing Footprint	A7S (SF)
18 (AF)	Stand-off Indirect Fire	A7C (CE)
19 (AF)	Sniper Attack	A7S (SF)
20 (AF)	Hostage Crisis	A7S (SF)
21 (AF)	Contamination of Drinking Water System	SG3 (Medical)
22 (AF)	Extended Loss of Energy Supply	A7C (CE)
Note: Scenarios are numbered to correspond to the national scenarios, except for AF added scenarios		

2.7.3. Tailor AT plans to the level of command or activity for which the AT principles were developed. AT plans may reference information from installation contingency response plans. At a minimum AT plans shall address:

2.7.3.1. The minimum essential AT program elements (AT Standard 1) and standards prescribed by this instruction.

2.7.3.2. Specify risk correction or mitigation measures to establish a local baseline defensive posture. The local baseline defensive posture shall facilitate systematic movement to and from elevated security postures, including the application of RAMs.

2.7.3.3. AT physical security measures (Standard 13).

2.7.3.4. AT risk mitigation measures for AF off-installation facilities, housing and activities (Standard 15).

2.7.3.5. AT risk mitigation measures for HRP (Standard 16).

2.7.3.6. AT construction and building considerations (Standard 17).

2.7.3.7. AT risk mitigation measures for logistics and other contracting (Standard 18).

2.7.3.8. AT risk mitigation measures for critical asset security (Standard 19).

2.7.3.9. AT risk mitigation measures for in-transit movements.

2.7.3.10. AT incident response measures (Standard 20).

2.7.3.11. Terrorism consequence management measures, including CBRNE and weapons of mass destruction (WMD) mitigation planning (Standard 21 and CEMP 10-2).

2.7.3.12. FPCON implementation measures, including site-specific AT measures (Standard 22).

2.7.4. GCCs provide AT planning information (e.g., airfield, port and movement route information and criticality, threat and VA data) to deploying DOD units; and, directs the execution of advance site reviews to facilitate the AT planning process in areas where the assessed TTL is SIGNIFICANT or HIGH or where a specific Terrorism Warning is in effect.

2.7.4.1. At the discretion of the GCC, such security efforts may be waived for deployments or visits to controlled locations such as existing military installations. Augmentation of assessment personnel may be necessary to enable subordinate AF Component commanders to discharge their responsibility to provide security, surveys, assessments, CI and countersurveillance support, and to act as the liaison with the country team, host-nation security force, contractors and port authority.

2.7.5. In countries where available, AFOSI special agents are assigned to FP Detachments (FPD) and provide FP and CI services to in-transit DOD personnel. FPDs are mandated to provide surveys, assessments, CI and countersurveillance support, and act as the liaison with the country team, host-nation security forces, contractors and port authority.

2.7.6. Coordinate AFOSI support for large exercises, contingencies and special events in foreign countries.

2.7.7. Ensure plans include procedures to expedite off-base first and emergency responders onto the installation during increased FPCON.

2.8. Standard 8: AT Program Coordination.

2.8.1. GCCs coordinate AT and security matters with the appropriate CoM and host-nation authorities for countries within their AOR and with the Heads of the other DOD Components whose personnel are stationed in or transit the respective GCC AOR.

2.8.2. AF Component commanders of personnel who will be stationed in or transit the AOR of a GCC shall:

2.8.2.1. Initiate coordination of AT matters with the appropriate GCC pursuant to the requirements established by DODD 2000.12. The senior deployed commander with AT responsibility will designate an ATO in writing to coordinate with the AF Component to the GCC and provide this information through the Unit Deployment Centers with Unit Type Codes (UTCs) assigned for the deployment. AF elements of in-transit forces with less than 300 personnel and not deploying as a larger troop movement will comply with the GCC operation order (OPORD) and file an in-transit AT plan. File in-transit AT plans with their ATO and commander for approval. Coordinate with AF Components to GCCs or MAJCOMs to determine in-transit AT plan filing requirements. The plan will cover travel from permanent station to the initial assembly or embarkation point, where it becomes the responsibility of the senior officer of a larger movement, such as a troop commander. If the movement does not join a larger force where AT responsibility is transferred, the AT plan must include transit to the deployed location where a commander is designated as having AT responsibility by orders. For countries where the AF will be performing temporary duty, commanders will immediately contact the AFOSI unit or ATO responsible for that AOR. AFOSI will provide a specific, tailored threat briefing prior to departure.

2.8.2.1. **(DOVERAFB)** When a Wing deployment exceeds 300 personnel, the designated deployment ATO will be responsible for preparing an in-transit AT plan.

2.8.2.2. To support AT planning and implementation, AT matters are coordinated with local, State, Federal and host-nation authorities pursuant to existing law, and AF and DOD policy.

2.8.2.2. **(DOVERAFB) 436 AW/JA.** All Memorandums of Agreement (MOAs) and Memorandums of Understanding (MOUs) for Dover AFB shall be reviewed by the Installation AW/AT, 436 AW/SJA and a functional area expert annually.

2.8.3. Subordinate elements of the DOD Components on AF installations or self-supported separate facilities and AF tenant units on installations or self-supported separate facilities shall coordinate AT program and plan requirements with the host installation or self-supported separate facility commander or civilian equivalent director. Tenant units shall participate fully in installation and self-supported separate facility AT programs. At locations where there are multiple DOD components, such as DOD-leased facilities or other facilities where DOD occupies space, the designated senior DOD Component, unless otherwise stipulated by the applicable GCC, shall be responsible for integrating and coordinating individual DOD component security plans into a comprehensive installation, self-supported separate facility or area-wide AT program.

2.8.3. **(DOVERAFB)** Host-Tenant agreements will include provisions to ensure both DoD and non-DoD tenants comply with Installation AT/FP program requirements.

2.9. Standard 9: AT Officer (ATO).

2.9.1. Commanders will designate ATOs in writing (see Standard 26 for certification criteria). The ATO is the commander's military or civilian advisor charged with managing the AT Program. The ATO advisory role does not replace a functional manager's or commander's responsibility to execute programs in support of the operational commander's mission. Security clearance requirements will be established by the commander. ATOs shall be assigned to:

2.9.1.1. Installations or self-supported separate facilities with inherent responsibility for emergency response functions.

2.9.1.2. Wings and higher.

2.9.1.3. Squadrons having 100 or more personnel.

2.9.1.3. **(DOVERAFB)** All organizations/agencies on the Installation with more than 25 assigned personnel to include tenants and other DoD agencies, must appoint, in writing, a primary and alternate Unit AT Representative (must be an E-5 or above) to serve as the Unit AT/FP subject matter expert and advisor for the unit or agency. Once the primary and alternate Unit AT Reps have been appointed, units will forward their letters to the Wing AT office. The appointment letter will contain their full names, last 4 of SSANs, security clearances, duty phone numbers, e-mail addresses, and Level II AT Awareness Instructor training date. As a minimum, all Unit AT Reps must complete AT Level II computer based training course (**ttp://www.dss.mil/training/enrol.htm**) within 60 days of appointment. Commanders and agency chiefs

2.9.1.3.1. **(Added-DOVERAFB)** All Unit AT Reps will develop and maintain a Unit AT Continuity Book containing current copies of the following items:

2.9.1.3.1.1. **(Added-DOVERAFB)** Appointment letter(s).

2.9.1.3.1.2. **(Added-DOVERAFB)** Wing/Unit RAM Schedules (provided by Wing AT office).

2.9.1.3.1.3. **(Added-DOVERAFB)** AT Form 2, Random Antiterrorism Measure Tracking Sheet (Attachment 13).

2.9.1.3.1.4. **(Added-DOVERAFB)** Level I Training Documentation (Attachment 14).

2.9.1.3.1.5. **(Added-DOVERAFB)** Level II training certificate(s).

2.9.1.3.1.6. **(Added-DOVERAFB)** AT Self-Inspection Program (maintain on file for 24 months).

2.9.1.3.1.7. **(Added-DOVERAFB)** Facility Information (i.e., Bomb Threat Evacuation Plan, Shelter In-Place Procedures, Active Shooter Response Plan).

2.9.1.3.1.8. **(Added-DOVERAFB)** Basic Unit level AT Plan or OI.

2.9.1.3.1.9. **(Added-DOVERAFB)** Wing FPCON Checklists.

2.9.1.3.1.10. **(Added-DOVERAFB)** Unit-specific FPCON Checklists.

2.9.1.3.1.11. **(Added-DOVERAFB)** Publications/plans pertaining to AT, at a

minimum: DOD Directive 2000.12, DoD Directive 2000.16, DoD 2000.12H, AFI 10-245, AMC Sup 1 to AFI 10-245, Dover Sup 1 to AFI 10-245, Wing AT Plan 10-245 and Integrated Defense Plan, OPlan 31-101.

2.9.1.4. Deploying squadrons and higher with potential perimeter security and access control responsibilities.

2.9.1.5. Deploying units under the operational control of a designated commander having 300 or more personnel (both civilian and military) assigned.

2.9.2. All ATOs shall:

2.9.2.1. Assist the commander in implementing Joint, DOD, GCC and Air Force AT-related doctrine, policy and TTPs. Make recommendations to the commander if supplemental policy and guidance is necessary to execute the commander's AT Program.

2.9.2.2. Provide guidance, priorities and resourcing strategies for the correction or mitigation of AT vulnerabilities utilizing CVAMP.

2.9.2.3. Recommend CbT-RIF submissions to correct or mitigate emergency or emergent AT vulnerabilities through the AF Component to the GCC in accordance with Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5261.01F, *Combating Terrorism Readiness Initiatives Fund*.

2.9.2.4. Provide AT considerations, to include real-world and exercise lessons learned, into appropriate concept of operations and other procedural guidance.

2.9.2.5. Collaborate with the TWG to determine if action through warnings, policy and guidance or organize, train and equip functions are necessary based on worldwide terrorism incidents or threats.

2.9.2.6. Work closely with AFOSI and Security Forces to support and advocate the Air Force Eagle Eyes program.

2.9.3. The following are additional responsibilities for ATOs appointed based on paragraphs 2.9.1.1 (installation or self-supported separate facilities) and 2.9.1.2 (wings and higher):

2.9.3.1. The minimum grade of these ATOs shall be O-3, E-7, GS-12 or YA-02. At small units or deployed locations, where the rank requirements cannot be met, the priority for selecting an ATO should be based on AT expertise and certification.

2.9.3.2. ATOs will be assigned to the commander's immediate staff for unfettered access to the commander or a senior officer on the commander's immediate staff. For expeditionary units, the ATO is assigned to the headquarters staff of the senior commander assigned AT responsibility.

2.9.3.3. Ensure CVAMP is used to identify and track AT resourcing actions and appropriate vulnerabilities are submitted to the GCCs for funding assistance.

2.9.3.4. Ensure CVAMP is populated with AT-related assessment vulnerabilities in accordance with this instruction. Additional functional databases may be used for follow-on project information and tracking, but a reference note must be documented in the vulnerability observation within CVAMP. Coordinate with functional commanders to ensure AT-related vulnerabilities are entered in and decisions or actions are tracked in

CVAMP. **Note:** Other databases may be used to manage the follow up action(s), but the initial vulnerability and the project identification code or numbers must be recorded and tracked in CVAMP.

2.9.3.5. Monitor Program Element Code (PEC) 28047 and coordinates funding for AT initiatives.

2.9.3.6. Facilitate the ATWG and ATEC.

2.9.3.7. Coordinate with FPI representatives to develop the commander's CCIRs and PIRs.

2.9.3.8. Coordinate with Exercise Evaluation Teams (EETs) or the ATWG for integrated multifunctional, interagency (local, state, federal), OCONUS – multinational, installation-wide AT exercises involving AT, EM and/or Medical response per functional guidance to test capabilities against adversary COA, e.g., force on force, TTPs. The ATO assists functional leads in executing required exercises and evaluation of AT-related capabilities.

2.9.3.8. **(DOVERAFB)** The 436 AW/ATO and alternates will be designated as Trusted Agents for the purpose of developing and exercising AT scenarios as part of the Installation exercise and evaluation process. Ensure AT exercises are integrated into the Wing/base exercise schedule and at a minimum, tested/evaluated annually.

2.9.3.9. Coordinate multifunctional teams of Subject Matter Experts (SMEs) when conducting AT assessments. In conjunction with functional commanders, provide countermeasure(s) solutions to correct or mitigate risk or recommend where the commander may assume risk.

2.9.3.10. Assist CE in determining the design basis threat to meet AT construction standards based on local threats.

2.9.3.11. A full-time multi-functional staff shall be designated, trained and resourced to support these ATOs in administering their respective AT programs. As a minimum, functional representatives will be designated in writing. **Note:** AT programs should be integrated with other FP programs and overarching efforts to achieve protection, such as critical infrastructure protection and continuity of operations; however AF CIP is a separate AF program and restraint should be exercised if these program responsibilities are added to ATO responsibilities without appropriate SME staff support.

2.9.4. The following are additional responsibilities for ATOs appointed based on paragraph 2.9.1.1 (installation or self-supported separate facilities):

2.9.4.1. In conjunction with other ATOs, unit AT representatives, functionals and SMEs, facilitate interaction for developing and implementing plans and programs that allows seamless capability application and resource deconfliction for contingency response and incident management. As a minimum, this includes the AT, CEMP 10-2, MCRP, IDP and Disease Containment Plan (DCP).

2.9.4.2. Provide oversight to wing/installation RAM programs.

2.9.4.3. **(Added-DOVERAFB)** In addition, the Installation ATO will:

2.9.4.3.1. **(Added-DOVERAFB)** Disseminate AT/FP advisories, intelligence summaries, warnings, training information and policy guidance.

2.9.4.3.2. **(Added-DOVERAFB)** Advise the Installation Facilities Board, Integrated Defense Council, and Emergency Management Working Group on AT/FP matters.

2.9.4.3.3. **(Added-DOVERAFB)** Represent the Wing Commander at various meetings and forums (e.g., State Homeland Security Council, DHS Critical Infrastructure, etc.)

2.9.4.3.4. **(Added-DOVERAFB)** Lead AT Criticality Assessments and prepare a prioritized listing of assets for 436 AW/CC review.

2.9.4.3.5. **(Added-DOVERAFB)** Schedule and coordinate a Higher Headquarters assessment or conduct a local vulnerability and risk assessment annually IAW DoDI 2000.16.

2.9.4.3.6. **(Added-DOVERAFB)** Prepare the Random Installation Entry Vehicle Inspection RAMs (as directed by FPCON Normal Measure 2.1) schedules quarterly and provide to SFS for execution. These RAMs will be annotated in the daily SFS Blotter. Wing AT office will monitor/track RAMs for compliance.

2.9.4.3.7. **(Added-DOVERAFB)** Serve as the Wing OPR for the Force Protection Working Group (FPWG) and lead the Terrorism Vulnerability Assessment.

2.9.4.3.8. **(Added-DOVERAFB)** Serve as a core member of the Threat Working Group (TWG) and assume Chair duties during the absence of the SF/CC.

2.9.5. The following are additional responsibilities for ATOs appointed based on paragraphs 2.9.1.3 (squadrons over 100 personnel) and 2.9.1.4 (deploying squadrons) and responsibilities of Unit AT Representatives:

2.9.5.1. Ensure FPCONs are implemented and report status to the installation or self-supported separate facility ATO as prescribed in the installation or self-supported separate facility AT plan.

2.9.5.1. **(DOVERAFB)** Unit AT Reps will advise their commander and monitor their unit for FPCON implementation. The Unit AT Rep should work closely with the Unit Control Center (UCC) to ensure directed FPCON measures are fully executed within unit areas and report status to the Installation Control Center (ICC)/Crisis Action Team (CAT).

2.9.5.2. Participate in the ATWG and TWG.

2.9.5.3. Ensure functional TTPs and guidance are integrated with the installation or self-supported separate facility AT program.

2.9.5.4. Arrange for Level I - AT Awareness Training and pre-deployment country threat briefs if not provided through the Unit Deployment Center.

2.9.5.4. **(DOVERAFB)** Ensure all assigned military and civilian employees complete AT Level I training within 90 days of arrival on station, and thereafter, complete AT Level I Awareness refresher training annually. AT Level I training is conducted through the Advanced Distributed Learning System (ADLS) available through Air Force Portal at

https://golearn.csd.disa.mil/kc/main/kc_frame.**asp** for Air Force military and civilians and the Defense Technical Information Center at https

2.9.5.5. Assist in scheduling and tracking RAM implementation and provide this information to the installation or self-supported separate facility ATO as prescribed in local guidance.

2.9.5.5. **(DOVERAFB)** Ensure RAMs are conducted in accordance with current distributed Wing RAM listing and report problems to Wing AT office.

2.9.5.6. Assist in developing and tracking in-transit AT plans (Standard 8).

2.9.5.7. **(Added-DOVERAFB)** In addition, Unit AT Reps will:

2.9.5.7.1. **(Added-DOVERAFB)** Report to the Wing ATO for initial training and program overview within 60 calendar days of appointment.

2.9.5.7.2. **(Added-DOVERAFB)** Communicate/disseminate relevant AT information to unit personnel in a timely manner.

2.9.5.7.3. **(Added-DOVERAFB)** Prepare a Unit AT operating instruction and Unit AT Continuity Book IAW this supplement.

2.9.5.7.4. **(Added-DOVERAFB)** Initiate work orders, recommend policy, or otherwise assist in mitigating identified unit vulnerabilities as required. Coordinate AF Form 332s (CE Work Orders) with unit Facility Managers, as needed.

2.9.5.7.5. **(Added-DOVERAFB)** Review proposed renovations and new construction within the unit for compliance with AT standards per UFC 4-010-01.

2.9.5.7.6. **(Added-DOVERAFB)** Conduct an annual review of the Wing AT plan and this supplement or as required.

2.9.5.7.7. **(Added-DOVERAFB)** Ensure a Self-Inspection of the unit's AT program is conducted semiannually (NOTE: Wing-directed Self-Inspections are conducted during the months of April and October each year). Unit AT reps will utilize the 436 AW Unit Antiterrorism Program Self-Inspection Checklist provided by the 436 AW/AT office. The Unit Commander or Agency Chief will sign the Self-Inspection memorandum; Unit AT Reps will maintain a written record of Self-Inspections for at least 24 months within the Unit AT Continuity Book.

2.10. Standard 10: AT Working Group (ATWG).

2.10.1. Multi-functional ATWGs shall be established at installations and self-supported separate facilities and higher (stationary and deployed) that meet at least semi-annually or more frequently, depending upon the level of threat activity. ATWGs oversee the implementation of the AT Program, develop and refine AT plans and address emergent or emergency AT program issues. The ATWG recommends COAs to the ATEC; develops AT-related policy, TTP and guidance; clarifies AT roles and responsibilities; conducts long-range planning and recommends resourcing requirements; and addresses emergent or emergency requirements through CbT-RIF.

2.10.1. **(DOVERAFB)** The Wing ATO will schedule, record and facilitate the FPWG meetings. NOTE: DAFB's FPWG constitutes the Antiterrorism and Critical Infrastructure working groups.

2.10.2. ATWG membership shall include the ATO, the commander (or a designated representative), representatives of the principal staff, including persons with CBRNE expertise, tenant unit representatives and other representatives as required to support AT planning and program implementation. The chair and mandatory members of the ATWG will be designated in writing by the commander. Security clearance requirements for members will be established by the commander. An ATWG charter or similar document should be developed to describe member responsibilities and minimum functional and SME participation.

2.10.2.1. **(Added-DOVERAFB)** The AT Working and Critical Infrastructure Protection (CIP) Working Group have been combined on Dover AFB to form a Force Protection Working Group (FPWG). The FPWG is chaired by the 436 MSG/CD and will meet semi-annually or as needed. The FPWG serves as the Installation focal point for identifying Installation vulnerabilities, and developing plans, policy, and physical methods of mitigating or eliminating vulnerabilities. The FPWG will also identify and prioritize funding requirements for projects or equipment needed in support of the Installation's AT and CIP programs. The FPWG will report Installation vulnerabilities, mitigation, elimination or recommendation risk acceptance as well as funding requirements to the Installation Commander and Force Protection Executive Council (FPEC).

2.10.2.2. **(Added-DOVERAFB)** Specialized or ad-hoc FPWG meeting may be called/convened at the Chair's or Wing ATO's discretion and will meet as needed to address specialized or unique AT/FP issues, concerns, or requirements. Examples of issues working groups may be formed to address include but are not limited to: FPCON checklists, Core Vulnerability Assessment Management Program (CVAMP), barrier planning, and Commander's Initiative Fund proposals, etc. When formed, subject matter experts (SMEs) from appropriate disciplines may be added to supplement the FPWG. These personnel do not require formal appointment and will participate only as long as the ad-hoc working group is needed.

2.10.2.3. **(Added-DOVERAFB)** The FPWG is Chaired by the Deputy Commander, 436th Mission Support Group (436 MSG/CD). Members of the FPWG are subject matter experts in their functional area and represent their respective commanders as decision-makers on AT/FP issues. Refer to the FPWG charter (Attachment 10) for specific roles and responsibilities. Membership of the Dover FPWG includes:

1. Wing Antiterrorism Advisor (ATA)	2. Public Affairs (PA)
3. AF Office of Special Investigations (AFOSI)	4. Force Support Squadron (FSS)
5. Communications (CS)	6. Wing Plans (XP)
7. Civil Engineer (CE) a. {Operations & Readiness}	8. Medical Group (MG) a. {Public Health &

	Bioenvironmental}
9. Intelligence (IN)	10. Operations Group (OG)
11. Security Forces (SF)	12. Maintenance Group (MXG)
13. Financial Management (FM)	14. 512th AT NCO (512 SFS)
15. Contracting Squadron (CONS)	16. Critical Infrastructure Protection (ATC)
17. Judge Advocate (JA)	18. Tenants and other agencies

2.10.3. AF/A7SO chairs the Headquarters AF (HAF) FP Working Group.

2.10.3.1. **(Added-DOVERAFB)** Units/agencies directed to participate in the FPWG will appoint a primary and alternate FPWG member (Company Grade Officer, E-7 and above, or civilian equivalent) with at least a Secret clearance, in writing to the 436 AW/AT office using properly formatted memorandum. NOTE: Because specific expertise is required to formulate viable plans, projects, and recommendations, some units may require more than one functional representative.

2.11. Standard 11: Threat Working Group (TWG).

2.11.1. A multi-functional TWG shall be established at the installation and self-supported separate facilities and higher (stationary or deployed) that meet at least quarterly or more frequently, depending upon the level of threat activity. TWGs develop and refine terrorism threat assessments and coordinate and disseminate threat warnings, reports and summaries. The TWG reviews, coordinates and disseminates threat warnings, reports and summaries. They should consider terrorist threats and their asymmetrical methods of organization, intelligence, planning and operations that could pose a threat to the installation or operations in the Base Boundary and/or Base Security Zone (BSZ). They also track CBRN active defense warnings and intelligence community threat alerts and advisories regarding terrorist groups and analyze the applicability to the installation and its operations.

2.11.1. **(DOVERAFB)** The DAFB Threat Working Group (TWG) is organized IAW the Charter (Attachment 11). The TWG is the Installation Commander's primary focal point for identifying immediate threats to the Installation and will meet at least quarterly. The TWG will gather, analyze, and disseminate terrorist threat information and develop recommended courses of action to mitigate or counter such threats.

2.11.2. TWG membership shall include the ATO, the commander (or a designated representative), members of the staff, and appropriate representatives from tenant units, direct-hire, contractor, local, State, Federal, host-nation law enforcement agencies and the intelligence community. The chair and mandatory members of the TWG will be designated in writing by the commander. Security clearance requirements for members will be established by the commander. A TWG charter or similar document should be developed to describe member responsibilities and minimum functional and SME participation.

2.11.2. **(DOVERAFB)** The 436 SFS Commander has been designated as the Chair of the TWG. The following are core TWG members; SF Operations, Wing AT Advisor, AFOSI, OG/Intel and MDG (PHEO). Ad hoc members of the TWG consist of; 436 CS, 436

CES/CEX, 436 CES/EOD, 436 MDG (Public Health & Bioenvironmental), 512 AW/ATO and 512 AW/IN. The Installation Commander or TWG Chair may add members from other agencies such as 436 FSS, 436 AW/PA, and 436 AW/JA (not all inclusive) as appropriate, to enhance the TWG or address specific threats or COAs. The TWG normally meets once a month or as directed by the Chair.

2.11.3. Based on threat information, appropriate SMEs shall be assembled to provide information needed to develop predictive intelligence and recommend COA to counter threats or otherwise reduce risk. If resources are available, especially at high threat locations or at MAJCOM or higher levels, members of the TWG may be further organized to form the basis of an Intelligence Fusion Cell as described in AFTTP 3-10.2, *Integrated Base Defense Command and Control.*

2.12. Standard 12: AT Executive Committee (ATEC).

2.12.1. An AT executive-level committee or similarly structured corporate body will be established at the installation and self-supported separate facility level and higher (stationary or deployed) that meets at least semi-annually. ATECs develop and refine AT program guidance, policy and standards; act upon recommendations of the ATWG and TWG; and determine resource allocation priorities to mitigate or eliminate terrorism-related vulnerabilities. The chair and mandatory members of the ATEC will be designated in writing. Security clearance requirements for members will be established by the commander. An ATWG charter or similar document should be developed to describe member responsibilities and minimum functional and SME participation.

2.12.1. **(DOVERAFB)** All AT/FP issues should be closely coordinated with the Force Protection Executive Council (FPEC). The FPEC consists of senior members of the Installation Commander's staff. The task-organized composition should be tailored to provide the appropriate level of oversight for the Dover AFB AT program and plan. The FPEC will review Installation-wide AT/FP programs, open CVAMP items, AT/FP related plans, budget submissions, and provide recommendations to the 436 AW/CC for approval/disapproval.

2.12.1.1. **(Added-DOVERAFB)** The FPEC meets semi-annually or as directed by 436 AW/CC.

2.12.1.2. **(Added-DOVERAFB)** Membership of the FPEC will include:

2.12.1.2.1. **(Added-DOVERAFB)** Voting Members: 436 AW/CC, 436 AW/CV, 436 MSG/CC, 436 MXG/CC, 436 OG/CC, 436 MDG/CC, 436 AW/DS and 512 AW/CC.

2.12.1.2.2. **(Added-DOVERAFB)** Non-Voting Members: 436 MSG/CD, 436 SFS/CC, 436 CES/CC, 436 CS/CC, Wing ATA, AFOSI Det 306, 436 AW/PA, 436 OSS/CC, 436 OG/OGI, 512 MSG/CC, 512 AW/ATO, AFMAO, and any members of the FPWG applicable to the scheduled discussion.

2.12.2. AF/A7S chairs the HAF FP Steering Group.

2.13. Standard 13: AT Physical Security Measure.

2.13.1. Principles of AFTTP 3-10.1, *Integrated Base Defense*, AFI 31-101 and DOD 5200.08-R, *Physical Security Program*, are applied and fully integrated into AT plans to

ensure employment of a holistic security system to counter terrorist capabilities. Well-designed physical security measures are multi-layered and include the integration and synchronization of the following essential elements, as further described in DOD AT Standard 13: detection, assessment, delay or denial, communication and response. The development of comprehensive physical security measures requires the integration of facilities, physical security equipment, trained personnel, biometrics entry control equipment, when established, and procedures oriented at a minimum in support of perimeter and area security, access and egress control, protection against CBRNE attacks (including those using the postal system), HRP protection, barrier plans and facility standoff distances.

2.13.2. AOR or other mission-specific security policies are developed to guide subordinate development of local physical security systems and the purchase of physical security equipment.

2.13.3. Tenant command and unit security plans and measures are coordinated and integrated into the AT Plan.

2.13.3. **(DOVERAFB)** Commanders of squadron level units will prepare and post on 436AW/AT EIM site individual unit physical security plans and measures as part of the Unit's AT Plan IAW the Unit Antiterrorism Program Operating Instructions. Unit plans will be submitted to 436 AW/AT for review on an annual basis. Units with contingency response plan requirements (e.g., Security Forces, Medical, and Civil Engineer) may incorporate this into existing plans as long as all elements are addressed.

2.13.3.1. **(Added-DOVERAFB)** Major tenant units (Det 306 AFOSI, AAFES, DeCA, AFMAO, AFME, JPED and 512 AW) will prepare plans IAW agency guidance and provide an updated copy to 436 AW/AT annually.

2.13.4. Ensure barrier plans include measures to prevent reverse entry though exit lanes. Ensure the barrier plan affords personnel time to recognize a possible threat and employ the final barrier(s) while minimizing risk to vehicle occupants, e.g. placing a serpentine between the integrated defense (ID) check point and the final denial barrier. The purpose of the final denial barrier is to prevent an attack but planners must factor that most instances requiring barrier employment are because of mistakes in judgment by vehicle operators.

2.13.4.1. Barrier plans should protect facilities listed in the AT plan from vehicle attacks. Installations will ensure proper standoff through UFC and DOD O-2000.12-H recommended passive barriers. Barriers plans should also identify owner/users tasked with erecting barriers and specified time periods. See JP 3-07.02 for additional guidance on establishing barriers plans.

2.13.4.1. **(DOVERAFB)** The Installation Barrier Placement Plan is contained within the Wing AT Plan, Part 3 (OPlan 10-245).

2.14. Standard 14: Random Antiterrorism Measure.

2.14.1. The RAM program is developed and implemented as an integral component of the overall AT program and guided by the principles outlined in DOD O-2000.12-H. To maximize the effectiveness and deterrence value, RAMs should be implemented without a set pattern, either in terms of the measure selected, time, place or other variables. Lessons learned have highlighted unpredictability in security activities as one of the best and most

cost effective deterrents available to a commander. Randomly changing AT TTPs enable integrated defenses to appear formidable and prevent threats from easily discerning and predicting patterns or routines that are vulnerable to attack. RAMs, at a minimum, shall consist of the random implementation of higher FPCON measures, to include MAJCOM or locally developed site-specific measures, in consideration of the local terrorist capabilities. Random use of other security measures should be used to supplement FPCON measures. The RAM program shall be included in AT plans.

2.14.2. When developing and implementing an effective installation RAM process:

2.14.2.1. Include tenant units and tenant commands.

2.14.2.2. Implement daily RAMs to include weekends and holidays. The frequency will be increased as the threat increases. At least three RAMs chosen from higher FPCONs are required daily.

2.14.2.2.1. **(Added-DOVERAFB)** All units, agencies and tenant organizations assigned to Dover AFB are required to comply with and participate in the Wing Random Antiterrorism Measure (RAM) program. Unit Commanders or Agency Chiefs are responsible for ensuring compliance with the Wing RAM program. The Wing RAM program seeks to deter terrorist attacks on DoD facilities and personnel by varying security routines and bolstering our daily protective measures. These increased actions help obscure the security posture or "foot print" of our installation. RAMs introduce uncertainty to the Installation's overall security program to defeat terrorist surveillance and make it difficult for a terrorist to accurately predict our actions. This is accomplished by employing measures from higher Force Protection Conditions (FPCONs) to supplement the current FPCON measures already in place.

2.14.2.2.2. **(Added-DOVERAFB)** Unit AT Representatives have been designated OPRs for the execution of Wing-directed RAMs. In addition to the Wing-directed RAMs, Units/agencies are required to employ a unit or functional specific RAM once a week. Document both measures using the DAFB AT Form 2, RAM Tracking Sheet (Attachment 12). In the event the RAM cannot be conducted at the directed time because personnel are not on duty, contact the AT office for a supplemental measure, and date and annotate the AT Form 2 with a detailed reason for non-compliance. Maintain the AT Form 2 in the Unit AT Continuity Book and forward a copy to the Wing AT office within 2 duty days of completing RAMs.

2.14.2.2.3. **(Added-DOVERAFB)** A minimum of two non-Security Forces related Wing RAMs will be accomplished daily. The 436 AW/AT office will send 90-day Wing RAM listings to Unit AT Representatives. The 436 AW/CC has delegated approval authority to the Wing AT Officer.

2.14.2.3. Use RAMs to mitigate vulnerabilities impacting facilities and nearby areas.

2.14.2.4. RAM implementation should be compatible and coordinated with ongoing law enforcement or CI surveillance detection and ID measures.

2.14.2.5. Consider methods to make RAMs visible to confuse or expose surveillance attempts and preoperational planning.

2.14.2.6. Implement dynamic and proactive RAMs to communicate unit resolve to detect, deter, prepare for and counter threats.

2.14.2.7. Make efforts to include, as appropriate local, State, Federal and host nation law enforcement patrols and first responders.

2.14.2.8. Implement RAMs installation wide or target specific types of facilities, functions or activities.

2.14.2.9. RAM implementation efforts shall be monitored, tracked and analyzed.

2.14.2.9. **(DOVERAFB)** Unit AT Representatives will annotate completed Wing-directed RAMs on the DAFB AT Form 2 RAM Tracking Sheet (Attachment 12) and provide them to the 436 AW/AT office on the 2nd of each month or first duty day following a weekend.

2.14.2.9.1. **(Added-DOVERAFB)** Unit AT Representatives will maintain a copy of completed DAFB AT Forms 2 within their Unit AT Rep Continuity Book for at least 12 months.

2.15. Standard 15: AT Measures for AF Off-Installation Facilities, Housing and Activities.

2.15.1. For AF owned or leased off-installation facilities, housing, transportation services, daycare centers and other activities used by or involving a mass-gathering of DOD personnel and their family members, specific AT measures shall be developed in overall AT programs. At locations where there are multiple DOD components or locations, AT measures shall be coordinated with the designated senior DOD Component with AT responsibility.

2.15.1.1. Risk mitigation measures shall include, but are not limited to: emergency notification and recall procedures, guidance for selection of off-installation housing, temporary billeting and other facility use (including compliance with UFC 4-010-01 for leased, newly constructed and expeditionary buildings), physical security measures, CBRNE defensive measures and shelter-in-place, relocation and evacuation procedures.

2.15.1.2. **(Added-DOVERAFB)** Local off-base Hotel Assessments will be coordinated, scheduled, tracked, and lead by the 436th Force Support Squadron (FSS). Prior to the 436th Contracting Squadron issuing any new Blanket Purchase Agree (BPA) for off-base lodging, a comprehensive facility assessment will be conducted by a cross-functional team of subject matter experts (SMEs); AFOSI, AT, Contracting, Fire Dept, FSS, Public Health and SFS will ensure the facility is acceptable for occupancy by DoD personnel. In addition, the cross-functional team will also conduct a formal assessment every 5 years to recertify the BPA.

2.15.1.2.1. **(Added-DOVERAFB)** Each cross-functional SME will develop a standardize checklist for their functional area. These checklists will be used during off-base Hotel Assessments and results will be provided to the FSS lodging representing heading the initial BPA review or recertification. All checklists will be reviewed annually and provided to the Wing AT office.

2.15.1.2.2. **(Added-DOVERAFB)** Security specialists from AFOSI, SFS and AT have developed a Hotel Assessment Security Checklist (Attachment 18) for use during Hotel Assessments. 436 SFS/S2 (Force Protection Intelligence) is designated

as the Wing security lead to conduct Hotel Assessments (initial and 5 year recertification) and will consult with AFOSI and AT, if needed.

2.15.1.2.3. **(Added-DOVERAFB)** All off-base lodging BPAs require an annual review/recertification. During annual off-base lodging follow-up assessments; the FSS representative will utilize the Hotel Assessment Security Checklist and report any unacceptable conditions immediately to the Contracting Squadron, applicable base agencies and the 436 SFS/S2 if a security issue is identified. All off-base Hotel Assessment reports will be submitted to the Contracting Squadron for inclusion into the facility BPA folder.

2.15.2. Mutual Aid Agreements or other similarly structured protocols are developed with the appropriate local, State, Federal and host-nation authorities to coordinate security measures and assistance requirements.

2.16. Standard 16: AT Measures for High-Risk Personnel (HRP).

2.16.1. AT measures are developed pursuant to the principles outlined in DOD O-2000.12-H, DODI O-2000.22 and AFI 71-101, vol 2, *Protective Service Matters,* for personnel designated as HRP.

2.16.1.1. SAF/IGX is the HAF focal point for policy development and coordination with the OASD for Special Operations and low-Intensity Conflict and Interdependent Capabilities (OASD (SO/LIC&IC)) to implement DODI O-2000.22.

2.16.1.2. AFOSI is designated a PPO and is the AF lead for Protective Service Details (PSDs) and PSVAs.

2.16.2. Designation of positions as High-Risk Billets (HRB) and HRP shall be in accordance with DODI O-2000.22 and AFI 71-101, vol 2.

2.16.2.1. SAF/IGX shall staff nomination packages for the Secretary of the Air Force (SECAF), who will make the decision to nominate AF officials to the Office of the Secretary of Defense (OSD).

2.16.2.2. SAF/AA shall staff nomination packages for the AF Top-4 as appropriate.

2.16.2.3. Nomination packages shall be staffed through the appropriate MAJCOM or AF Component to a GCC.

2.16.3. AFOSI will complete a PSVA for each person occupying an HRB who is nominated for HRP in accordance with DODI O-2000.22 and AFI 71-101, vol 2. PSVAs will be initiated within 90 days of an individual's assignment to an HRB and nomination for HRP. PSVA will be revalidated annually and updated if the TTL changes, but no less than every 3 years.

2.16.4. HRP and family members, as appropriate, shall complete appropriate high-risk training (personal protection, evasive driving, AT awareness and hostage survival); shall be properly cleared for assignment to positions, facilities or countries requiring such protection; and shall be thoroughly indoctrinated on the duties and responsibilities of protective service personnel.

2.16.5. HRP designees and their family members shall be familiar with treaty, statutory, policy, regulatory and local constraints on the application of supplemental security measures

for certain high-ranking DOD officials who are provided additional protection due to their position.

2.16.6. HRP security measures shall be reviewed within 60 days of changes to the TTL for the affected country and HRP.

2.16.7. The provisions of AFI 23-302, *Vehicle Management,* shall be complied with for the acquisition and use of non-tactical armored vehicles.

2.17. Standard 17: AT Construction and Building Considerations.

2.17.1. All new construction and renovations, regardless of the funding source, that exceed 50 percent of the replacement cost or change the use of the facility must comply with UFC 4-010-01, *DOD Minimum Antiterrorism Standards for Buildings*. Refer to AFPD 31-1, AFI 31-101, AFI 65-601, Vol 1, *Budget Guidance and Procedures*, and AFH 32-1084, *Facility Requirements*, for additional information. Proper facility project planning, programming and design must be done in concert with the ATO, installation intelligence and security personnel to adequately address site specific threats. Ensure restoration and modernization projects which include security and AT Standards compliance upgrades do not exceed 70 percent cost versus new facility standard.

2.17.1.1. The installation commander or the senior Civil Engineer on the commander's behalf will certify that new facility or renovation projects of 50 percent or more of replacement cost comply with standards as listed in paragraph 2.17.1. The ATO will work with the engineering staff from design inception to project completion, ensuring requirements are met. The ATO should be part of the coordination prior to certification. The senior Civil Engineer will report discrepancies to the appropriate MAJCOM for determination/action.

2.17.1.1. **(DOVERAFB)** The 436 CES will ensure the Wing ATO is notified of facility construction and rehabilitation projects and afforded an opportunity to attend appropriate planning meetings in their earliest possible stages. Facility related AT enhancements will be submitted to the 436 CES via an AF Form 332, Civil Engineer Work Request. Facility modification or additional work requests will be reviewed by the Unit AT Representative for compliance with UFC 4-010-01, *DoD Minimum Antiterrorism Standards for Buildings*, prior to submittal to the 436 CES. Project priorities for AT will be approved by the Facilities Board and/or FPEC.

2.17.1.2. **(Added-DOVERAFB)** The 436 CES will certify that new facility or renovation projects comply with AT minimum standards.

2.17.2. Ensure the A7 (CE) and ATO develop a prioritized list of risk mitigation measures (reference DOD O-2000.12-H, UFCs and AFI 31-101) for use by site selection teams. These criteria shall be used to determine if facilities either currently occupied or being considered for occupancy provide adequate protection for DOD personnel against the effects of a terrorist attack. Circumstances may require the movement of DOD personnel or assets to facilities the U.S. Government had not previously used or surveyed. AT Standards shall be a key consideration in evaluating the suitability of facilities that were previously not used or surveyed.

2.17.3. The A7 (CE) will ensure at least one engineer at each installation has completed the Security Engineering and Design Course to review, document and track construction projects for compliance with UFCs and AT Standards.

2.17.3. **(DOVERAFB)** The 436 CES will identify at least one engineer who has received Security Engineering and Design Course training as the AT Project POC. The AT Project POC must provide their certificate of training to 436 AW/AT.

2.18. Standard 18: AT Measures for Logistics and Other Contracting.

2.18.1. AT measures shall be incorporated into the logistics and contracting processes (requirements development, vendor selection, award, execution and evaluation) when the provisions of the contract or services provided affect the security of DOD elements, personnel, mission-essential cargo, equipment, assets or services. When commensurate with risk, consider AT performance as an evaluation factor for contract award (past performance and proposed performance under the instant contract) and as a performance metric under the resultant contract.

2.18.1. **(DOVERAFB)** AT contract considerations will be jointly developed by 436 CONS and 436 AW/AT, and incorporated into AT and ID Plans.

2.18.2. A verification process, whether through background checks or other similar processes shall be implemented to enable the U.S. Government to attest to the trustworthiness of DOD contractors and sub-contractors (U.S. citizens, host-nation and third country personnel) to the greatest extent possible, including those personnel having direct or indirect involvement in the delivery or provision of services. Priority will go to service provisioning related to mail and food, water or other materiel intended for consumption by DOD personnel. This vetting of trustworthiness shall include agents and crews on contracted ships, planes, trains and overland vehicles. Refer to AFI 31-101.

2.18.3. Site-specific risk mitigation measures are developed and implemented to maintain positive control of DOD contractor and sub-contractor access to and movement within installations, sensitive facilities and classified areas.

2.18.4. Site-specific risk mitigation measures are developed and implemented to screen contractor or sub-contractor transportation conveyances for CBRNE hazards before entry into or adjacent to areas with DOD personnel and mission-essential assets.

2.18.5. Contracts will comply with the AT provisions of the Defense Federal Acquisition Regulation.

2.18.6. Contracts shall incorporate Level I - AT Awareness Training requirements. See Standard 25.

2.19. Standard 19: AT Measures for Critical Asset Security.

2.19.1. Risk management measures shall be developed to reduce the vulnerabilities of DOD assets assessed as critical in STANDARD 5, to include distributive information or computer-based systems and networks. Integrate these measures into overall AT program efforts.

2.19.1. **(DOVERAFB)** AT risk management measures will be included in the AT Plan.

2.19.2. Coordinate with appropriate local, State, Federal or host-nation authorities responsible for the security of non-DOD assets deemed essential to the functioning of DOD assets assessed as critical.

2.20. Standard 20: Terrorism Incident Response Measures.

2.20.1. Incident response measures shall be developed consistent with the principles outlined in DOD 5200.08-R and AFI 10-2501 and included in the overall AT plan. These measures shall include procedures for determining the nature and scope of incident response (including incidents with a CBRNE component); procedures for coordinating security, fire, medical, hazardous material and other emergency responder capabilities; and steps to recover from the incident while continuing essential operations.

2.20.1. **(DOVERAFB)** Terrorist Incident Response Measures are contained within the AT Plan, and synchronized or referenced in various adjunct plans including the Comprehensive Emergency Management Plan (CEMP 10-2), Medical Contingency Response Plan (MCRP), and the IDP.

2.20.2. AF Components to GCC or GCCs prepare incident response measures for their AOR. AFOSI and Force Protection Detachments should be included in contingency planning for in-transit units.

2.21. Standard 21: Terrorism Consequence Management Measures.

2.21.1. Consequence management, CBRNE and public health emergency preparedness and emergency response measures are included as an adjunct to the overall AT Plan or installation emergency management plans. For the AF these measures are found in the CEMP 10-2, MCRP, AT Plan and the IDP. The contents of all plans may be referenced in the AT Plan. These measures shall focus on mitigating vulnerabilities of personnel, families, facilities and materiel to terrorist use of WMD and CBRNE weapons, as well as overall disaster planning and preparedness to respond to a terrorist attack. These measures shall include integration with DOD emergency responder guidelines provided in AFI 10-2501; mass notification system standards under UFC 4-021-01; establishment of medical surveillance systems consistent with DODD 6490.02E, *Comprehensive Health Surveillance*, and AFI 10-2604, *Disease Containment Planning Guidance*; deployment of CBRNE sensors and detectors; providing collective protection; and providing personal protective equipment (PPE) or individual protective equipment (IPE) in the following priority and in accordance with AFI 10-2501. The contract Statement of Work or Performance Work Statement must specify if PPE will be government or contractor provided:

2.21.1. **(DOVERAFB)** Terrorist Consequence Management Measures are contained within the AT Plan, and synchronized or referenced in various adjunct plans including CEMP 10-2, MCRP, and the IDP.

2.21.1.1. First Responders and Emergency Responders. Personnel who work closest to known or suspected CBRNE hazards (e.g., emergency responders) should be provided protection needed to perform their duties in an unknown hazard environment. Responders should use the maximum possible protection until determined otherwise by competent authority.

2.21.1.2. Critical Personnel. Personnel deemed essential to the performance of critical military missions (whether military, civilian, contractor, host-nation personnel or third country nationals), such as critical personnel assigned to mission essential functions (MEFs) described in AFI 10-208, *Continuity of Operations Program (COOP)*, should be provided an appropriate level of protection to support continuity of those critical military

missions. Since critical missions should be continued without interruption, collective or individual protection may be necessary to sustain them.

2.21.1.3. Essential Personnel. Personnel deemed essential to the performance of essential military operations (whether military, civilian, contractor, host-nation personnel or third country nationals) should be provided an appropriate level of protection to support near continuity for those essential military operations. Since essential operations may be interrupted for relatively short periods (e.g., hours to days), escape protection may be necessary to sustain essential operations (i.e., escape, survive and restore essential operations).

2.21.1.4. Other Personnel. For all other persons not in the above categories, the objective will be to provide the procedures or protection necessary to safely survive an incident, e.g. shelter-in-place or evacuation procedures may fulfill this requirement.

2.21.1.5. Included as part of the above categories are those who work or live on DOD installations worldwide, family members authorized overseas and DOD contractors if designated in contract agreements and designated as essential to perform critical DOD missions.

2.21.2. Site-specific CBRNE preparedness and emergency response measures are developed and coordinated through the Readiness and Emergency Management Flight. These measures are implemented and synchronized with a corresponding FPCON measure.

2.21.3. Mutual Aid Agreements or other similarly constructed protocols will be established with the appropriate local, State, Federal or host-nation authorities to support AT Plan execution and augment incident response and post-incident consequence management activities.

2.21.4. The installation should be able to warn its resident population in affected areas of possible or confirmed CBRNE hazards immediately, utilizing the Air Force Installation Notification and Warning System (INWS). The warning must include instructions to shelter in place or evacuate.

2.21.5. Installation public health emergency response measures that are synchronized with FPCON levels shall be developed and implemented.

2.22. Standard 22: Force Protection Condition (FPCON) Measures.

2.22.1. The GCC is responsible for establishing the baseline FPCON for their AOR and procedures to ensure that FPCON measures are uniformly disseminated and implemented. The AF Component to the GCC is typically delegated to manage this task for the GCC. See Attachment 2 for detailed listing of FPCON measures.

2.22.2. Installation commanders with AT responsibility and higher shall:

2.22.2.1. Determine an appropriate FPCON level for those personnel and assets for which they have AT responsibility. Subordinate commanders may raise a higher-level commander's FPCON level, but they shall not lower the FPCON level without the higher-level commander's written concurrence.

2.22.2.1. **(DOVERAFB)** Raising or lowering FPCON will only occur when directed by the 436 AW/CC, CAT Director (when the ICC is activated) or Wing succession of

command. However, in some instances a local contingency action or security incident can trigger the automatic implementation of an increased FPCON IAW the Integrated Defense Plan, 31-101.

2.22.2.2. Classify site-specific AT measures and physical security actions, linked to an FPCON as "CONFIDENTIAL". When separated from the AT Plan, specific AT measures linked to a FPCON and site-specific FPCON levels may be downgraded to "FOR OFFICIAL USE ONLY," in accordance with DOD 5200.1-R, *Information Security Program*.

2.22.3. A review mechanism is established to ensure FPCON levels are commensurate with changing threats and the principles of risk management. This is essential because implementation of FPCON measures at elevated FPCON levels for an extended duration can be counterproductive to effective security and overall mission accomplishment. In some circumstances, based upon local conditions and the threat environment, commanders should consider implementing a lower-level FPCON and supplement with other local security measures and RAMs as an effective alternative to executing the higher-level FPCON measures.

2.22.3. **(DOVERAFB)** The DAFB TWG will review local FPCON measures annually and make recommendations to the Installation Commander through the Force Protection Executive Committee (FPEC) when conditions and principles of risk management warrant adjustment.

2.22.4. Site-specific FPCON measures are developed and implemented for stationary and in-transit forces to supplement the FPCON measures and actions enumerated for each FPCON level. The development of site-specific FPCON measures must permit sufficient time and space to determine hostile intent, while fully considering constraints imposed by standing rules of engagement in CJCSI 3121.01B, *Standing Rules of Engagement/Standing Rules For the Use of Force For U.S. Forces,* and rules of force under AFI 31-207, *Arming and Use of Force by Air Force Personnel*. Organic intelligence, CI and law enforcement resources, institutional knowledge of the area and comprehensive understanding of organic capabilities, supported by national and AOR assets, shall be leveraged in directing tailored FPCON measures to be implemented at specific sites for both stationary and in-transit forces.

2.22.4. **(DOVERAFB)** Site-specific measures and actions set for each FPCON are included as part of the AT Plan, but are produced and maintained under separate cover to keep them "For Official Use Only" IAW AFI 10-245.

2.22.4.1. **(Added-DOVERAFB)** All available mass media will be utilized to assist in disseminating FPCON changes to include unit and installation electronic marquees, Commander's Access Channel, e-mail, computer log-on banners, telephone alerting system, Giant Voice, etc.

2.23. Standard 23: AT Training and Exercises.

2.23.1. AT training and exercises shall integrate with physical security and relevant elements of AT, EM, FHP and ID and are afforded the same emphasis as combat task training and executed with the intent to identify shortfalls affecting the protection of personnel, assets and information against terrorist attack and subsequent AT consequence management efforts.

2.23.2. AT and AOR specific training, particularly pre-deployment training, is supported by measurable standards, including credible deterrence and response standards, deterrence-specific TTPs and lessons learned. AT training shall also be incorporated into unit-level training plans and pre-deployment exercises. Pre-deployment training shall also include terrorism or similarly designed scenarios and hostile intent decision making. Joint operations and exercises shall incorporate AT training and planning for forces involved.

2.23.3. At least annually, comprehensive field and staff training, including deploying squadrons and higher, are conducted to exercise AT plans. Annual AT exercises shall encompass all aspects of AT, physical security and emergency management plans. Additionally, current baseline FPCON through FPCON CHARLIE measures shall be exercised annually at installations and self-supported separate facilities.

2.23.4. Maintain AT exercise documentation for no less than 2 years to ensure incorporation of lessons learned.

2.23.5. AT lessons learned are submitted through the AF Lessons Learned program and, when appropriate, through the Joint Lessons Learned program.

2.23.6. ATOs in coordination with the Wing EET shall develop a comprehensive annual training and exercise program to provide the necessary individual and collective training to prepare for an annual exercise.

2.23.6. **(DOVERAFB)** Base exercises will be directed by the Wing Exercise Manager, 436 AW/XPE, and conducted by the Installation Exercise Evaluation Team (EET). AT exercises may be combined with other base contingency exercises (e.g., Initial Response Readiness Exercise, Emergency Management Exercise). The 436 AW/CV, through XPE, will conduct annual Installation level AT exercises to evaluate AT plans. AT exercises will ensure planned scenarios test the full spectrum of FPCON implementation, evacuation procedures, notification plans, terrorist use of Weapons of Mass Destruction (WMD), and other key areas of the AT Plan as identified by the 436 AW/ATO. Furthermore, simulations will be held to an absolute minimum to allow thorough testing of the Installation's response actions to a terrorist attack or acts of terrorism.

2.24. Standard 24: Formal AT Training.

2.24.1. The AF's formal AT Training Program shall consist of Level 1 - AT Awareness Training (Standard 25), Level II - ATO Training (Standard 26), Level III - Pre-command AT Training (Standard 27), Level IV - AT Executive Seminar (Standard 28), AOR-specific training (Standard 29) and HRP AT training (Standard 16).

2.24.2. AT training shall be integrated into officer, NCO and civilian training as required by this Instruction and whenever possible and appropriate. Long term improvement and implementation of effective AT programs depends upon a solid training foundation for all grades, skills and functional areas.

2.24.2.1. All AF assigned personnel shall complete appropriate formal AT training and education. Individual permanent records shall be updated to reflect completion of the training.

2.24.2.2. ATOs and unit personnel are encouraged to attend additional protection related courses, e.g., Security Engineering and Design Course.

2.24.2.3. Required AT formal training shall be provided to individuals who are not properly trained upon arrival to a new assignment or as soon as possible. Report AF training deficiencies through the AF chain of command to the appropriate MAJCOM. Report other Service training discrepancies through the appropriate AF Component to the GCC.

2.25. Standard 25: Level I - AT Awareness Training.

2.25.1. Every military Service member, DOD employee and local national or third country citizen in a direct-hire status by the DOD, regardless of grade or position, shall complete Level I - AT Awareness Training requirements.

2.25.1. **(DOVERAFB)** Active duty and Reserve Air Force members and DoD employees in a direct-hire status must complete initial and annual AT Level I Awareness Training. The primary training source is through the Advanced Distributed Learning System (ADLS) available through AF Portal at https://golearn.csd.disa.mil/kc/main/kc_frame.asp?blnWhatsNew=True. This site automatically records completion and enables the user to print a certificate if needed (e.g., to attach to an Individual Antiterrorism Travel Plan). Level I training for contractors and dependents may be accomplished through DTIC at https://atlevel1.dtic.mil.

2.25.2. DOD contractors shall be provided AT information as required by DFAR, Section 252.225-7043. Level I - AT Awareness Training shall be offered to DOD contractor employees under the terms and conditions as specified in the contract, especially when the performance is OCONUS. The TWG should determine the best method to offer training to contractor employees.

2.25.3. Dependent family members ages 14 years and older traveling OCONUS on official business (e.g., on an accompanied permanent change of station move) shall complete Level I - AT Awareness Training as part of their pre-departure requirements.

2.25.3. **(DOVERAFB)** Commander's will encourage all inbound PCS dependents of military or DoD personnel (14 years of age and older) to complete AT Level I Awareness Training during unit in-processing, annually thereafter, and prior to any OCONUS travel. Sponsors may facilitate Level I training for family members.

2.25.3.1. Commanders will encourage dependent family members to complete Level I - AT Awareness training before any personal travel OCONUS (e.g., leave) or to any locale where the TTL is MODERATE or higher.

2.25.4. Level I - AT Awareness Training shall be provided in initial entry basic training or in general military subject training for all initial entry AF military and civilian personnel. AF personnel accessions must receive this initial training under the instruction of a qualified Level I - AT Awareness Training instructor.

2.25.5. All individuals qualified to administer Level I - AT Awareness Training will be designated in writing. Individuals who complete a formal AF approved Level II - ATO Training (Standard 26) course of instruction, whether in residence or through a mobile training team, may qualify to administer Level I - AT Awareness training.

2.25.5.1. If a certified instructor is not available, as an interim solution, commanders will certify and appoint qualified SMEs (e.g., security forces, special agents, EM, Bioenvironmental Engineer, intelligence personnel) who have received formal training in

AT TTP and individual security and protection, and are knowledgeable in the current AT publications and methods for obtaining AOR-specific updates. Commanders must clearly describe the qualifications of the individual in the appointment letter to justify this method and explain why other options are not feasible.

2.25.6. Individuals completing Level I - AT Awareness Training shall:

2.25.6.1. Have the requisite knowledge to remain vigilant for possible terrorist actions.

2.25.6.2. Be capable of employing AT TTP as outlined in DOD O-2000.12-H.

2.25.7. Level I - AT Awareness Training is built upon the minimum requirements outlined in DODI 2000.16, Standard 25, Table E3.T2. Table 2.2 below supplements DOD Standard 25 with AF modifications. AT Awareness training offered by other Services or DOD agencies meets AF requirements as long as they fulfill all requirements of DOD Standard 25.

Table 2.2. Minimum AT Awareness Training Requirements.

AT Awareness instruction shall include at least the following subjects (AF added/modified):
- Personal protective measures for CBRNE attacks utilizing local or theater specific emergency management guidance and procedures
- Force Health Protection measures

2.25.8. Annually, post-accession Level I - AT Awareness Training shall be provided to all AF personnel. Annual post-accession Level I - AT Awareness Training may be accomplished by one of two means:

2.25.8.1. Instruction from a qualified Level I AT Awareness Training instructor.

2.25.8.2. Completion of a DOD or AF-sponsored and certified computer or web-based distance learning instruction. **Note:** AF personnel assigned or attached to an embassy on TDY under CoM authority must receive Level I – AT Awareness Training from a qualified instructor.

2.25.9. HQ AF Security Forces Center (AFSFC/SFOZ) is responsible for managing the AF Level I - AT Awareness Training.

2.25.10. AF assigned personnel complete Level I – AT Awareness Training as part of the AF annual ancillary training program.

2.25.10.1. The Force Support Squadron will document Level I - AT Awareness Training for individuals and their dependents that are 14 years or older. This training requirement will be included in the relocation process. Training must be completed prior to final out-processing.

2.25.10.2. Orders approving officials and/or Unit Deployment Managers (UDM) shall document completion of Level I - AT Awareness and AOR specific training on OCONUS deployment orders.

2.25.10.2. **(DOVERAFB)** Unit Deployment Managers (UDMs) will ensure personnel projected for OCONUS TDY are current in Level I AT Awareness Training prior to deployment and document this training in the members' individual mobility folders.

2.25.10.3. Unit Training Managers document Level I - AT Awareness Training with the date of completion in Military Modernization Personnel Data System (MILPDS). If MILPDS is unavailable, Unit Training Managers will document AT Awareness Training through normal ancillary records. Unit Training Managers will provide Level I - AT Awareness Training status and statistics upon request.

2.25.10.4. Aircrews will document their Level I - AT Awareness Training as ARMS Code G110 (Level I - AT Awareness Training).

2.26. Standard 26: Level II - ATO Training.

2.26.1. Individuals will be qualified as an ATO by completion of a formal AF approved Level II - ATO Training course of instruction, whether a course in residence or through a mobile training team. At permanent duty locations, newly assigned, uncertified ATOs shall complete a formal AF approved Level II - ATO Training course within 120 days of appointment. At temporary duty locations the most expedient arrangements shall be used to send a trainee to formal training.

2.26.1. **(DOVERAFB)** AT Level II training is required for Installation level Antiterrorism Officers and personnel appointed to the Threat Working Group, Force Protection Working Group, and Unit AT Representatives. Scheduling of all Level II in-residence or Mobile Training Team (MTT) training must be coordinated through the 436 AW/AT office. Alternately, Level II computer based training is available through the Defense Security Service (DSS) by enrolling at the following location: http://www.dss.mil/training/enrol.htm

2.26.2. AF approved Level II - ATO Training courses are listed in Attachment 5. Level II - ATO Training shall prepare ATOs to manage AT programs, advise the commander on all AT issues, qualify individuals to administer Level I - AT Awareness Training and coordinate support required for completion of Level I - AT Awareness Training.

2.26.3. Certified ATOs shall remain current and proficient.

2.26.3.1. Personnel who are qualified as an ATO but have not served as an ATO in the last 12 months shall complete a formal AF approved Level II - ATO refresher training course of instruction. The refresher may be through a course in residence, mobile training team or computer or web-based distance learning instruction.

2.26.3.2. Personnel who are qualified as an ATO but have not served as an ATO in the last 13 months to 3 years shall re-attend a formal AF approved Level II - ATO Training course of instruction. The refresher may be through a course in residence or mobile training team.

2.26.3.2.1. **(Added-DOVERAFB)** Unit AT Reps will re-accomplish AT level II training after 3 years (36 months) have passed since initial certification. The re-certification may be accomplished through formal in-residence training, mobile training team (MTT) or computer/web-based distance learning course (i.e. DSS Academy).

2.26.4. MAJCOMs with Level II - ATO Training courses shall:

2.26.4.1. Designate course of instruction requirements for ATO personnel.

2.26.4.2. For new courses, submit a Plan of Instruction (PoI) to HQ AFSFC/SFOZ for approval prior to initiating any training. PoIs will be submitted to HQ AFSFC/SFOZ as requested.

2.26.4.3. Command-specific requirements may be added to the core curriculum. Develop measurable standards for Level II - ATO Training and determine evaluation methods to ensure trainees are proficient.

2.26.4.4. Conduct an annual review of Level II - ATO Training course curriculum to validate minimum curriculum content.

2.26.4.5. Maintain a reference library of all AT-related publications relevant to the course of instruction.

2.26.4.6. Develop an AF Form 797, *Qualification Standard Continuation/Command Job Qualification Standard(JQS),* to task certify personnel serving as instructors, as appropriate.

2.26.4.7. Establish a PDS Code of "AFI" to identify Level II - ATO Training courses.

2.26.4.8. Review potential instructor candidates to ensure prerequisites are met prior to commencement of duties.

2.26.5. Personnel serving as Level II - ATO Training course instructors will, as a minimum, have completed the following:

2.26.5.1. A formal AF instructor's course, such as Principles of Instruction, Academic Instructor School, Basic Instructor Course, etc. The Principles of Instruction course is the minimum required standard. Personnel may begin instructing students without having completed this requirement provided they have a certified instructor serving as the Supervising Instructor. However, they are required to have a date to attend one of the above courses within 90 days of being assigned instructor duties.

2.26.5.2. Graduate from an AF approved Level II - ATO Training course (Attachment 5).

2.26.5.3. Be task certified on an AF Form 797, as appropriate.

2.26.5.4. Instructors should expand their AT knowledge by attending courses such as sister Service AT training, Dynamics of International Terrorism (DIT) and CVAMP training. Additionally, conducting over-the-shoulder observations of HHA VAs adds to credibility and subject matter expertise.

2.26.5.5. Level II - ATO Training instructors should have had 2-years field experience as an ATO.

2.26.6. Level II - ATO Training is built upon the minimum requirements outlined in DODI 2000.16, Standard 26, Table E3.T3. Table 2.3 below supplement DOD Standard 26 with AF modifications. The AF developed Level II - ATO Training courses can be specialized, but every course must cover either the installation (I) or deployable unit (U) joint requirements, at a minimum.

Table 2.3. Minimum Level II - ATO Training Requirements.

1. (I/U) Complete a formal AF-approved Level II - ATO Training course of instruction, whether a course in residence or through a mobile training team (CONUS or OCONUS).

2. (I/U) Level II - ATO Training shall consist of the following minimum topics (AF added):

a) (I/U) Understanding FP Roles and Responsibilities

- (I/U) Understand necessary Host Nation and Civil Support Agreements and Requirements

b) (I/U) Prepare AT Plans (consider using the JAT Guide)

- (U) How to Integrate AT Plans with CEMP 10-2, MCRP, IDP, etc.

3. (I/U) Review of the following DOD and Joint Staff publications (AF added).

a) (I/U) UFCs 4-010-01, 4-010-02, 4-020-01fa, 4-020-03fa, 4-020-04fa, 4-022-01, 4-023-03 and 4-021-01

b) I) Agile Combat Support Concept of Operations

c) (I) AFDD 2-4.1, *Force Protection*

d) (I/U) AFTTP 3-10.1, *Integrated Base Defense*

e) (I/U) AFTTP 3-10.2, *Integrated Base Defense Command and Control*

f) (I/U) AFI 10-245, *Antiterrorism (AT)*

g) (I/U) AFI 10-2501, *AF Emergency Management (EM) Program Planning and Operations*

h) (I) AFI 10-2603, *Emergency Health Powers on Air Force Installations*

i) (I) AFI 10-2604, *Disease Containment Planning Guidance*

j) (I/U) Air Force Lessons Learned Program

k) (I/U) AFI 14-119, *Intelligence Support to Force Protection*

l) (I/U) AFI 31-101, *The Air Force Installation Security Program*

4. (I/U) If available, add the following to Level II - ATO Training courses:

a) SME presentations from the Federal Bureau of Investigations (FBI), AFOSI, EOD, Intel, Medical Group, etc.

b) Hands-on instruction of Antiterrorism Enterprise Portal (ATEP) and CVAMP

2.27. Standard 27: Level III - Pre-command AT Training.

2.27.1. Squadron, group and wing commanders (O-5 or O-6 commanders and civilian equivalent director position) shall complete Level III - Pre-command AT Training before assuming command.

2.27.2. MAJCOMs will ensure this training is provided to squadron commanders, e.g. during MAJCOM squadron commander orientation seminars or other means. Group and wing commanders will receive this training through the group and wing commander courses. MAJCOMs will determine minimum qualifications for personnel delivering Level III - Pre-command AT Training.

2.27.3. Level III - Pre-command AT Training is built upon the requirements outlined in DODI 2000.16, Standard 27, Table E3.T4. Table 2.4 below supplement DOD Standard 27 with AF modifications. A minimum of a 1-hour block is provided to properly address the minimum topics. Additionally, commanders are encouraged to attend the Joint Special Operations School's "*Commander's Responsibility Course, Antiterrorism and Force Protection.*"

2.27.3.1. Installation commanders are required to gain a thorough understanding of all the requirements.

2.27.3.2. All other commanders are required to gain a thorough understanding of all requirements not marked with an asterisk. Asterisk designated requirements only require introduction, which at a minimum will include explanatory remarks and sufficient reference material for commanders to complete their AT responsibilities.

Table 2.4. Minimum Level III - Pre-command AT Training Requirements.

1. Pre-Command AT training shall include the following minimum topics (AF added/modified):
a) Understanding AT responsibilities and minimum AT Program Elements
- Risk Management and Risk Assessments
b) * Ensuring preparation of AT plans
- Baseline FPCON posture
- Integrated Defense Plan
- Mitigating CBRNE, WMD attack and risks in support of EM plans
- MOUs, Memorandums of Agreement (MOAs) and MAAs
- JAT Guide Capabilities
c) * Organization of AT groups
- ATWG
- TWG
- ATEC

d) *Understanding the local threat picture

- Potential sources of law enforcement-derived Force Protection information

- Fusion of Intelligence, CI and law enforcement information

- Terrorism Threat Levels

e) *How the installations integrate with the National Response Framework

f) *How the installation integrates with the Country Team

2. Review of references includes GCC OPORDs (AF added).

2.28. Standard 28: Level IV - AT Executive Seminar.

2.28.1. Commanders at all echelons will ensure appropriate military officers in the grades of O6 through O8 and civilian equivalent/senior executive service civilian employees attend the AT Executive Seminar as described in DOD Standard 28.

2.28.2. The AT Executive Seminar is administered by the Joint Staff (J-3 Deputy Director for AT/Homeland Defense, J34). Nomination requests are sent through the Services and COCOMs.

2.28.3. The AT Executive Seminar provides DOD senior military and civilian executive leadership with the requisite knowledge to enable development of AT Program policies and facilitate oversight of all aspects of AT programs at the operational and strategic levels.

2.29. Standard 29: Area of Responsibility (AOR)-Specific Training for DOD Personnel and In-transit Forces.

2.29.1. GCCs develop and provide AOR specific training and provide in-transit forces with threat information. The AT awareness training and education programs orient all DOD personnel with AOR-specific information on AT protection. This AOR-specific information is in addition to annual Level I - AT Awareness Training and may be provided through multiple means, including GCC/AF Component to the GCC/MAJCOM publications, messages, Internet Web sites, AFI 24-405 and DOD 4500.54-M.

2.29.1. **(DOVERAFB)** The 436 FSS Career Development office verifies personnel departing TDY, TDA, or PCS to OCONUS areas have received proper AT training. Unit Deployment Managers will ensure AOR-specific AT training is provided by OG/Intel, AFOSI and/or the member's respective Unit AT Representative.

2.29.2. AF personnel (including family members ages 14 years and older) departing to another GCC's AOR shall complete the gaining GCC's, AF Component to the GCC's or MAJCOM's AOR-specific AT education requirements within 3 months of a permanent change of station.

2.29.2. **(DOVERAFB)** Units will document compliance with AT training for individuals scheduled to OCONUS PCS or TDY by ensuring an Individual Antiterrorism Plan is completed prior to travel. Aircrew members receive AOR-specific threat/intelligence briefs, supplemental training if required and are exempt from this individual requirement.

2.29.3. Commanders of AF in-transit forces, units and individuals will obtain from GCCs, AF Component to the GCCs or MAJCOMs detailed threat information covering transit routes

and sites that will be visited by the deploying unit or individuals. Such information includes focused information on potential terrorist threats (e.g., tailored production and analysis) and guidance on the development of AT protection risk mitigation measures to aid in the development of tailored AT planning. Similar tailored information is also provided to intra-theater transiting units and individuals.

2.30. Standard 30: AT Resource Application.

2.30.1. Risk shall be assessed against the standard and mitigation measures applied. Where the resulting risk is still deemed too great, the countermeasure requirement shall be elevated using the PPB&E process. Where applicable and in accordance with the MOU between the Department of State (DOS) and the DOD, *Overseas Security Support*, coordination will be made through MAJCOMs or AF Components to GCCs with the appropriate GCC to ensure that resource requirements for AT programs are identified and programmed. See Attachment 4 for more information on AT resourcing.

2.30.2. For emergent or emergency AT requirements that could not reasonably have been anticipated or programmed, prioritization shall be coordinated with the appropriate GCC, AF Component to the GCC or MAJCOM and CbT-RIF requests shall be submitted to the Chairman of the Joint Chiefs of Staff (CJCS) as specified in CJCSI 5261.01E. AF Components to the GCC or MAJCOMs will submit CbT-RIF through the GCC. GCCs forward CbT-RIF requests to the CJCS using CVAMP.

2.30.3. MAJCOMs will submit validated prioritized AT resource requests with compelling justification, including those submitted or considered for CbT-RIF, to the GCC for review and submission to the CJCS on an annual basis pursuant to current DOD Program Objective Memorandum (POM) guidance and timelines using CVAMP.

2.30.4. Tenant units on AF installations and facilities shall coordinate and prioritize AT program and resource requirements according to PPB&E procedures with the host installation commander, applicable Military Department and appropriate GCC.

2.30.5. Antiterrorism PEC 28047F is the primary funding source for manpower authorizations, AT equipment, procurement, and the associated costs specifically identified and measurable to those resources and activities associated with the Air Force AT Program. AF/A7SX is the AF Program Element Monitor (PEM).

2.31. Standard 31: Comprehensive AT Program Review.

2.31.1. Comprehensive AT program reviews are conducted to evaluate the effectiveness and adequacy of AT program implementation. The evaluation shall include an assessment of the degree to which Air Force AT programs comply with the standards prescribed in this Instruction. AT program reviews shall evaluate all mandatory AT program elements (DOD Standard 1) and assess the viability of AT plans (DOD Standard 7) in view of local operational environment constraints and conditions. DOD O-2000.12-H provides procedures and recommendations to conduct comprehensive AT Program reviews. Other procedures include reviewing AT programs based on JSIVA or AFVAT benchmarks or DOD AT Strategic goals.

2.31.2. Comprehensive AT program reviews shall be conducted at least annually by all commanders required to establish AT programs.

2.31.2. **(DOVERAFB)** Annual AT Program Review: The Wing ATO will lead and administer the Wing's annual AT Program Review (PR). The PR will be accomplished using the HQ AMC/IG Unit Compliance Checklists (AMC/A7S Antiterrorism Checklist/PR Tool). The Wing ATO will ensure all functional areas (designated FPWG representatives) and Unit AT programs (all unit and tenant organizations) participate in the PR process. OPRs will be designated locally to review and validate compliance/non-compliance with each checklist item. The PR will normally be conducted in conjunction with the Wing-directed semi-annual Self Inspection (SI), initiated in April and October or as directed. The Wing AT office will task functional area OPRs and Unit AT Representatives to complete the checklist and submit a written report, indorsed by the Unit Commander or Agency Chief. The Wing AT office will compile the results and provide a formal memorandum to the Wing SI Manager (XP). The AT Mission Area SI results will be forwarded to the Wing Commander through XP. The completion of the SI fulfills the comprehensive annual Antiterrorism PR requirement. In addition, the Wing ATO will brief the Wing Commander of any critical program element(s) reported as non-compliant and consider for inclusion into CVAMP.

2.31.3. Comprehensive AT program reviews shall be conducted in conjunction with pre-deployment VAs (Standard 6).

2.31.3.1. The purpose of a pre-deployment AT program reviews is to ensure that deploying units have viable AT programs and executable AT plans for transit to, from and during operations or training exercises in the deployed AOR.

2.31.3.2. Deploying AF elements shall comply with the GCC's AT guidance.

2.31.4. A comprehensive AT program review shall be conducted whenever there are significant changes in threat, vulnerabilities or asset criticality.

2.31.5. MAJCOMs shall ensure subordinate commands undergo an external AT program review at least once every 3 years. The ultimate outcome of triennial AT program reviews is the identification of AT program deficiencies that may be exploited by terrorists. The AT program review teams should provide realistic solutions aimed at improving AT program implementation and risk mitigation strategies.

2.31.5.1. Triennial AT program reviews may be conducted as an HHA or JSIVA. The AF may use an HHA or JSIVA in lieu of an annual AT program review.

2.31.5.2. In addition to providing an assessment of compliance with the AT Standards, an HHA or JSIVA shall assess and evaluate the viability of a headquarters' AT policies, subordinate AT program implementation, the methodology for addressing resource shortfalls, inter-organization coordination and synchronization of AT program elements.

2.31.6. Tenant commands and units located on AF installations shall be included in comprehensive AT program reviews.

2.32. Standard 32: AT Program Review Teams.

2.32.1. AT program review assessment team guidelines shall be modeled upon the *DTRA AT VA Team Guidelines* and include, at a minimum, compliance with the standards prescribed in this Instruction, accepted TTPs and best AT practices.

2.32.2. A sufficient number of AT program review teams shall be resourced to execute the program review assessment requirements of the AF and to ensure AT program review teams

comprise of individuals with sufficient functional expertise to assess and evaluate satisfactorily the effectiveness and adequacy of AT Program implementation at the level for which the AT Program review is being conducted (headquarters, unit, command, installation, activity, etc.).

2.33. Adopted Forms.

AF Form 797, *Job Qualification Standard Continuation/Command JQS*

AF IMT 847, *Recommendation for Change of Publication*

DANIEL J. DARNELL, Lt Gen, USAF
DCS/Air Space and Information Operations, Plans and Requirements

(DOVERAFB)

MARK D. CAMERER, Colonel, USAF
Commander, 436th Airlift Wing

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFDD 2-4.1, *Force Protection*, 9 November 2004

AFPD 10-24, *Air Force Critical Infrastructure Program*, 28 April 2006

AFPD 10-25, *Emergency Management*, 26 September 2007

AFPD 10-26, *Counter-Chemical, Biological, Radiological and Nuclear Operations*, 26 September 2007

AFPD 31-1, *Integrated Defense*, 7 July 2007

AFPD 71-1, *Criminal Investigations and Counterintelligence*, 1 July 1999

AFI 10-208, *Continuity of Operations Program (COOP)*, 1 December 2008

AFI 10-246, *Food and Water Protection Program*, 4 December 2004

AFI 10-2501, *Air Force Emergency Management (EM) Program Planning and Operations*, 24 January 2007

AFI 10-2603, *Emergency Health Powers on Air Force Installations*, 7 December 2005

AFI 10-2604, *Disease Containment Planning Guidance*, 6 April 2007

AFI 14-119, *Intelligence Support to Force Protection (FP)*, 15 August 2007

AFI 23-302, *Vehicle Management*, 29 October 2007

AFI 24-405, *Department of Defense Foreign Clearance Guide*, 6 May 1994

AFI 31-101, *The Air Force Installation Security Program*, 1 March 2003

AFI 31-207, *Arming and Use of Force by Air Force Personnel*, 29 January 2009

AFI 33-200, *Information Assurance (IA) Management*, 23 December 2008

AFI 38-201, *Determining Manpower Requirements*, 30 December 2003

AFI 65-601volume 1, *Budget Guidance and Procedures*, 3 March 2005

AFI 71-101volume 1, *Criminal Investigation*, 1 December 1999

AFI 71-101volume 2, *Protective Service Matters*, 18 November 2002

AFI 90-201, *Inspector General Activities*, 22 November 2004

AFH 10-2401, *Vehicle Bomb Mitigation Guide* (FOUO), 1 September 2006

AFH 32-1084, *Facility Requirements*, 1 September 1996

AFMAN 10-2602, *Nuclear, Biological, Chemical, and Conventional (NBCC) Defense Operations and Standards*, 29 May 2003

AFTTP 3-10.1, *Integrated Base Defense*, 20 August 2004

AFTTP 3-10.2, *Integrated Base Defense Command and Control*, 1 March 2008

AFTTP 3-10.3, *Integrated Defense Counterthreat Operations (CTO)*, 22 December 2008

CJCS Guide 5260, *Antiterrorism Personal Protection Guide: A Self-Help Guide to Antiterrorism*, 1 February 2008

CJCSI 3121.01B, *Standing Rules of Engagement/Standing Rules For the Use of Force For U.S. Forces* (available on SIPR at **www.js.smil.mil/masterfile/sfsimd/jel/index.htm**)

CJCSI 5261.01F, *Combating Terrorism Readiness Initiatives Fund*, 21 October 2008

CJCS Pocket Card 5260, *Antiterrorism Individual Protective Measures*, 1 October 2001

DODD 2000.12, *DOD Antiterrorism (AT) Program*, 18 August 2003

DODD 3020.40, *Defense Critical Infrastructure Program (DCIP)*, 19 August 2005

DODD 4500.54-M, *DOD Foreign Clearance Manual (FCM)*, 16 December 2008 (**https://www.fcg.pentagon.mil/fcg.cfm**)

DODD 6490.02 E, *Comprehensive Health Surveillance*, 21 October 2004

DODI 2000.16, *DOD Antiterrorism (AT) Standards*, 2 October 2006; change 2, December 8, 2006

DODI O-2000.22, *Designation and Physical Protection of DOD High-Risk Personnel (HRP)*, 22 January 2008

DODI 4525.8_AF Supplement 1, *DOD Official Mail Management*, 20 March 2006

DODI 5210.89_AFI 10-3901, *Minimum Standards for Safeguarding Biological Select Agents and Toxins*, 24 September 2007

DODI 5240.18, *Counterintelligence Analysis and Production*, 4 December 2006

DOD O-2000.12-H, *Antiterrorism Handbook*, 1 February 2004

DOD O-2000.12-P, *Department of Defense Antiterrorism Strategic Plan*, 1 June 2004

DOD 5200.1-R, *Information Security Program*, 14 January 97

DOD 5200.08-R, *Physical Security Program*, 9 April 2007

DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons*, 1 December 1982

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 30 May 2008

JP 3-07-2, *Antiterrorism*, 14 April 2006

UFC 4-010-01, *DOD Minimum Antiterrorism Standards for Buildings*, 8 October 2003

UFC 4-010-02, *DOD Minimum Antiterrorism Standoff Distances for Buildings*, 8 October 2003

UFC 4-021-01, *Design and O&M: Mass Notification Systems*, 18 December 2002

Agile Combat Support Concept of Operations, October 1999

Defense Federal Acquisition Regulation Supplement (DFARS), 20 October 2008

Defense Threat Reduction Agency, *Antiterrorism Vulnerability Assessment Team Guidelines*, March 1, 2002

Defense Threat Reduction Agency (JSIVA) Security Classification Guide 6 May 2005

Homeland Security Presidential Directive 5, 28 February 2003

Homeland Security Presidential Directive 8, 17 December 2003

National Response Framework, January 2008

Protection Joint Functional Concept, June 2004

Unified Command Plan, 5 May 2006

Abbreviations and Acronyms

AF CIP—Air Force Critical Infrastructure Program

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

AFSFC—Air Force Security Forces Center

AFTTP—Air Force Tactics, Techniques and Procedures

AOR—Area or Responsibility

AT—Antiterrorism

ATEC—Antiterrorism Executive Committee

ATO—Antiterrorism Officer

ATWG—Antiterrorism Working Group

BSAT—Biological Select Agents and Toxins

NAF—Component-Numbered Air Force

CBRNE—Chemical, Biological, Radiological, Nuclear and high-yield Explosive

CbT—Combating Terrorism

CbT—RIF—Combating Terrorism Readiness Initiatives Fund

CCIR—Commander's Critical Information Requirements

CEMP—Comprehensive Emergency Management Plan

C&I—Communications and Information

CI—Counterintelligence

CJCS— Chairman of the Joint Chiefs of Staff

CJCSI— Chairman of the Joint Chiefs of Staff Instruction

COA—Course of Action

CoM—Chief of Mission

CONOPS—Concepts of Operations

CTO—Counterthreat Operations

CVAMP—Core Vulnerability Assessment Management Program

DCIP—Defense Critical Infrastructure Program

DCP—Disease Containment Plan

DFAR—Defense Federal Acquisition Regulation

DIA—Defense Intelligence Agency

DOD—Department of Defense

DODD—Department of Defense Directive

DODI—Department of Defense Instruction

DOS—Department of State

DRU—Direct Reporting Units

DTA—DOD Threat Assessment

EET—Exercise Evaluation Team

EM—Emergency Management

EOD—Explosive Ordnance Disposal

FHP—Force Health Protection

FOA—Field Operating Agency

FP—Force Protection

FP—Force Protection Detachment

FPCON—Force Protection Condition

FPI—Force Protection Intelligence

GCC—Geographic Combatant Commander

GSU—Geographic Separated Unit

HHA—Higher Headquarters Assessment

HAF—Headquarters Air Force

HN—Host Nation

HRB—High-Risk Billet

HRP—High-Risk Personnel

ID—Integrated Defense

IDP—Integrated Defense Plan

IED—Improvised Explosive Device

IPE—Individual Protective Equipment

JAT—Joint Antiterrorism Guide

JP—Joint Publication

JSIVA—Joint Staff Integrated Vulnerability Assessment

MAA—Mutual Aid Agreement

MAJCOM—Major Air Command

MCRP—Medical Contingency Response Plan

MEF—Mission Essential Functions

MILCON—Military Construction

NAF—Numbered Air Force

OASD—Office of the Assistant Secretary of Defense

OCONUS—Outside the Continental United States

OPCON—Operational Control

OPORD—Operation Order

OPR—Office of Primary Responsibility

PA—Public Affairs

PEC—Program Element Codes

PHEO—Public Health Emergency Officer

PIR—Priority Intelligence Requirement

POM—Program Objective Memorandum

PPB&E—Planning, Programming, Budgeting and Execution

PPO—Protection Providing Organization

PPE—Personal Protective Equipment

PSVA—Personal Security Vulnerability Assessment

RAM—Random Antiterrorism Measure

RED HORSE—Rapid Engineer Deployable Heavy Operations Repair Squadron

SME—Subject Matter Expert

SOFA—Status of Forces Agreement

TACON—Tactical Control

TIC—Toxic Industrial Chemical

TIM—Toxic Industrial Material

TTL—Terrorism Threat Level

TTP—Tactic, Technique and Procedure

TWG—Threat Working Group

UCP—Unified Command Plan

UFC—Unified Facilities Criteria

UTC—Unit Type Codes

VA—Vulnerability Assessment

VBIED—Vehicle Born Improvised Explosive Device

WMD—Weapons of Mass Destruction

Terms

Active Defense—The employment of limited offensive action and counterattacks to deny a contested area or position to the enemy.

Air Force Emergency Management (EM) Program—The single, integrated Air Force program to coordinate and organize efforts to prepare for, prevent, respond to, recover from and mitigate the direct and indirect consequences of an emergency or attack. The primary missions of the Air Force EM program are to (1) save lives, (2) minimize the loss or degradation of resources and (3) continue, sustain and restore combat and combat support operational capability in an all-hazards physical threat environment at Air Force installations worldwide. The ancillary missions of the Air Force EM program are to support homeland defense and civil support operations and to provide support to civil and host nation authorities IAW DOD directives and through the appropriate Combatant Command. The Air Force EM program is managed by the Office of The Civil Engineer, AF/A7C.

Antiterrorism (AT)—Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces.

Assessment—Analysis of the security, effectiveness and potential of an existing or planned intelligence activity. (JP 1-02) [The evaluation of progress toward the creation of effects and the achievement of objectives and end state conditions.][AFDD 2-1.9]{Words in brackets apply only to the Air Force and are offered for clarity.}

AT Awareness—Fundamental knowledge of both the terrorist threat and the measures to reduce personal vulnerability to terrorism.

AT Officer (ATO)—The principal military or civilian advisor charged with managing the AT program for the commander or DOD civilian exercising equivalent authority.

AT Planning—The process of developing specific guidance and execution-oriented instructions for subordinates. An AT plan contains command-specific guidance for the establishment of an AT program and the implementation of the AT Standards.

AT Program—One of several security-related programs that fall under the overarching combating terrorism and FP programs. The AT program is a collective, proactive effort focused on the prevention and detection of terrorist attacks against DOD personnel and their families, facilities, installations and infrastructure critical to mission accomplishment as well as the

preparation to defend against and planning for the response to the consequences of terrorist incidents. Although not elements of AT, plans for terrorism consequence management preparedness and response measures as well as plans for continuing essential military operations are important adjuncts to an effective AT program. The minimum elements of an AT program are AT risk management, planning, training and exercises, resource application and a program review.

AT Program Review—The process of developing specific guidelines used to evaluate the AT Program in order to assess satisfactorily and evaluate the effectiveness and adequacy of the AT Program.

AT Resource Application—The process of applying risk management to vulnerabilities and where the resultant risk is not acceptable after applying mitigation measures, elevate the vulnerability with a resource request using the existing PPB&E system, the CbT-RIF, the Physical Security Program and other funding mechanisms. Central to success in resource application is tracking and ensuring sufficient funding for identified AT program life-cycle costs and assessed shortfalls to mitigate risk associated with terrorist capabilities.

AT Risk Management—The process of systematically identifying, assessing and controlling risks arising from operational factors and making decisions that balance possible adverse outcomes with mission benefits. The end products of the AT program risk management process shall be the identification of DOD elements and personnel that are vulnerable to the identified threat attack means. From the assessment of risk based upon the three critical components of AT risk management (threat assessment, criticality assessment and vulnerability assessment), the commander must determine which DOD elements and personnel are at greatest risk and how best to employ given resources and FP measures to deter, mitigate or prepare for a terrorist incident.

AT Training and Exercises—The process of developing individual, leader and collective skills and of conducting comprehensive exercises to validate plans for AT incident response, consequence management and continuity of essential military operations.

Biological Select Agents and Toxins (BSAT)—Biological agents and toxins that present a high bioterrorism risk to national security and have the greatest potential for adverse public health impact with mass casualties of humans and/or animals or that pose a severe threat to plant health or to plant products. The lists are reviewed and updated by HHS/CDC and USDA/APHIS. Agents and toxins that are excluded in Title 42, Code of Federal Regulations, Part 73, and Title 7, Code of Federal Regulations, Part 331 are excluded as BSAT.

Combating Terrorism (CbT)—For the purposes of this Instruction, combating terrorism within the DOD encompasses all actions, including AT, counterterrorism, terrorism consequence management (preparation for and response to the consequences of a terrorist incident or event) and terrorism intelligence support (collection and dissemination of terrorism-related information), taken to oppose terrorism throughout the entire threat spectrum, including terrorist use of CBRNE.

Combating Terrorism Readiness Initiatives Fund (CbT-RIF)—Program established by Congress in the FY 1997 National Defense Authorization Act and managed by the J-3 DDAT/HD. Provides funds for emergency and emergent high-priority antiterrorism projects or equipment submitted by combatant commands and approved by the Chairman of the Joint Chiefs

of Staff or a designated representative, after coordination with the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict and the Services.

Commander—Personnel assigned to command positions at all levels and the heads of the Defense Agencies and DOD Field Activities.

Commander's Critical Information Requirements (CCIR)—An information requirement identified by the commander as being critical to facilitating timely decision-making. The two key elements are friendly force information requirements and priority intelligence requirements.

Comprehensive AT Program Review—The systematic assessment of the AT program against the AT Standards.

Consequence Management—For the purpose of this Instruction, consequence management is those measures taken to protect public health and safety, restore essential Government services and provide emergency relief to governments, businesses and individuals affected by the consequences of a CBRNE situation. For domestic consequence management, the primary authority rests with the States to respond. The Federal Government responds through the Department of Homeland Security's Federal Emergency Management Agency, as the Lead Federal Agency (LFA) for providing assistance as required. DOS is the LFA for foreign consequence management.

Coordination—The necessary action to ensure adequate exchange of information to integrate, synchronize and deconflict operations between separate organizations. Coordination is not necessarily a process of gaining approval but is most often used for mutual exchange of information. Normally used between functions of a supporting staff. Direct liaison authorized (DIRLAUTH) is used to coordinate with an organization outside of the immediate staff or organization.

Counterintelligence (CI)—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations or persons, or international terrorist activities.

Criminal Intelligence (CRIMINT)—Law enforcement information derived from the analysis of information collected through investigations, forensics, crime scene and evidentiary processes to establish intent, history, capability, vulnerability and modus operandi of threat and criminal elements.

Crisis Management—For the purpose of this Instruction, crisis management is those measures taken to resolve a hostile situation and to investigate and prepare a criminal case for prosecution under Federal law. Crisis management shall include a response to an incident involving WMD, a special improvised explosive device or a hostage crisis that is beyond the capability of the LFA.

Critical Asset—An asset that is of such extraordinary importance that its incapacitation or destruction would have a serious, debilitating effect on the ability of one or more DOD Components or Defense Infrastructure Sector Lead Agents to execute the task or MET it supports. TCAs are used to identify defense critical assets.

Criticality Assessment—For the purposes of this Instruction, an assessment of the effect of temporary or permanent loss of key assets or infrastructures on the installation or a unit's ability

to perform its mission. The assessment also examines costs of recovery and reconstitution including time, funds, capability and infrastructure support.

Defense Critical Asset—An asset of such extraordinary importance to DOD operations in peace, crisis and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the Department of Defense to fulfill its mission.

Defense Critical Infrastructure (DCI)—Department of Defense and non-Department of Defense networked assets and essential to project, support and sustain military forces and operations worldwide.

Deterrence—The prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction.

DOD AT Program—The minimum elements of the DOD AT program as a whole and of DOD Component AT programs are AT risk management, planning, training and exercises, resource application and program review.

DOD Civilian Work Force—U.S. citizens or foreign nationals working for the Department of Defense and paid from appropriated or non-appropriated funds under permanent or temporary appointment. This includes employees filling full-time, part-time, intermittent or on-call positions. Specifically excluded are all Government contractor employees.

DOD Component—The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the Department of Defense Agencies, field activities and all other organizational entities in the Department of Defense.

DOD Contractor—Any individual, firm, corporation, partnership, association or other legal non-Federal entity that enters into a contract directly with the Department of Defense to furnish services, supplies or both, including construction. Defense contractors may include U.S. nationals, local citizens or third country nationals. Defense contractors do not include foreign governments or representatives of foreign governments that are engaged in selling to the Department of Defense or a DOD Component or foreign corporations wholly owned by foreign governments.

DOD Elements and Personnel—For the purposes of this Instruction, DOD military and civilian personnel and their dependent family members; DOD contractors; DOD installations and facilities; DOD-owned, -leased or -managed defense critical infrastructure.

DOD Personnel—For the purposes of this Instruction, Uniformed Military Service members and DOD Federal civilian employees hired and paid from appropriated and non-appropriated funds under permanent or temporary appointment.

Eagle Eyes Program—A CSAF-approved Air Force antiterrorism defensive program created to enhance the collection of threat information by educating members of the Total Force and off-base citizens on the nature of terrorist attack-planning activities. The program also establishes 24-hour phone numbers to call when suspicious behavior is observed.

Emergency CbT-RIF Requirement—An unanticipated CbT-RIF requirement created by a combination of circumstances or the resulting state that requires IMMEDIATE action to prevent, deter or respond to a terrorist act.

Emergency Responders—Firefighters, law enforcement, security personnel, emergency medical technicians, emergency management and operations personnel, explosive ordnance disposal personnel, physicians, nurses, medical treatment providers at medical treatment facilities, disaster preparedness officers, public health officers, bioenvironmental engineers, counterintelligence agents and mortuary affairs personnel.

Emergent CbT-RIF Requirement—A newly-formed unexpected CbT-RIF requirement resulting as a logical consequence of unforeseen circumstances and calling for PROMPT action.

Facility—A real property entity consisting of one or more of the following: a building, a structure, a utility system, pavement and underlying land.

Family Member—Individuals defined as "Dependent" in section 1072(2) of title 10 U.S.C.

First Responder—Firefighters, law enforcement and/or security personnel, emergency medical technicians and EOD personnel (for suspected explosive CBRNE events) that provide the initial, immediate response to an accident, disaster, criminal, terrorist or CBRNE incident.

Food and Water Security—The protection of food and water sources from disruption and contamination or other terrorist acts that could severely impact operations. Food and water security measures include those actions taken to detect, prevent and mitigate the effects from intentional acts designed to disrupt or contaminate food and water sources.

Force Health Protection (FHP)—A comprehensive threat-based program directed at preventing and managing health related actions against Air Force uncommitted combat power.

Force Protection (FP)—Actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather or disease. (JP 1-02) [An integrated application of offensive and defensive actions that deter, detect, preempt, mitigate or negate threats against or hazards to Air Force air and space operations and assets, based on an acceptable level of risk.]{Definition in brackets applies only to the Air Force and is offered for clarity.}

Force Protection Condition (FPCON)—A DOD-approved system standardizing the Department's identification, recommended preventive actions and responses to terrorist threats against U.S. personnel and facilities. This system is the principal means for a commander to apply an operational decision on how to protect against terrorism. It facilitates inter-Service coordination and support for AT activities.

Force Protection Detachment (FPD)—A CI element that provides comprehensive CI support to transiting ships, personnel and/or aircraft in regions of elevated threat.

Force Protection Intelligence (FPI)—Analyzed, all-source information concerning threats to DOD missions, people or resources arising from terrorists, criminal entities, foreign intelligence and security services and opposing military forces. FPI supports FP decisions and operations

Foreign Intelligence—Information relating to capabilities, intentions and activities of foreign powers, organizations or persons, but not including counterintelligence, except for information on international terrorist activities. See also intelligence.

High-Risk Billet (HRB)—Authorized personnel billet (designated by the appropriate authority as identified in DODI O-2000.22) that because of grade (normally, General, Admiral or Senior Executive Service equivalent and assigned in a country with a DIA terrorist threat level of "Significant" or higher), assignment, travel itinerary or symbolic value may make a person filling it an especially attractive or accessible terrorist target.

High-Risk Personnel (HRP)—Personnel who, by their grade, assignment, symbolic value or relative isolation, are likely to be attractive or accessible terrorist targets.

Higher Headquarters Assessment (HHA)—An overall assessment by a higher headquarters of how an organization is managing its AT program, including management and compliance efforts by subordinate organizations.

Installation—A grouping of facilities, located in the same vicinity, which support particular functions. Installations may be elements of a base.

Installation Commander—The individual responsible for all operations performed by an installation.

Intelligence—The product resulting from the collection, processing, integration, evaluation, analysis and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity. See also acoustic intelligence; all-source intelligence; basic intelligence; civil defense intelligence; combat intelligence; communications intelligence; critical intelligence; current intelligence; departmental intelligence; domestic intelligence; electronic intelligence; electro-optical intelligence; foreign intelligence; foreign instrumentation signals intelligence; general military intelligence; human resources intelligence; imagery intelligence; joint intelligence; laser intelligence; measurement and signature intelligence; medical intelligence; merchant intelligence; military intelligence; national intelligence; nuclear intelligence; open-source intelligence; operational intelligence; photographic intelligence; political intelligence; radar intelligence; radiation intelligence; scientific and technical intelligence; security intelligence; strategic intelligence; tactical intelligence; target intelligence; technical intelligence; technical operational intelligence; terrain intelligence; unintentional radiation intelligence.

Joint Staff Integrated Vulnerability Assessment (JSIVA)—A vulnerability-based evaluation of an installation's ability to deter and/or respond to a terrorist incident. A vulnerability-based assessment considers both the current threat and the capabilities that may be employed by both transnational and local terrorist organizations, both in terms of their mobility and the types of weapons historically employed.

Mutual Aid Agreement—Written agreement between agencies, organizations, or jurisdictions that they will assist one another on request by furnishing personnel, equipment, or expertise in a specified manner. Reciprocal assistance by local government and an installation for emergency services under a prearranged plan. Mutual aid is synonymous with "mutual assistance," "outside aid," "memorandums of understanding," "memorandums of agreement," "letters of agreement," "cooperative assistant agreement," "intergovernmental compacts," or other similar agreements, written or verbal, that constitute an agreed reciprocal assistance plan for sharing emergency services. MAAs between entities are an effective means to obtain resources and should be

developed whenever possible. MAAs should be in writing, be reviewed by legal counsel and be signed by a responsible official.

Physical Security—For the purposes of this Instruction, that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material and documents; and to safeguard them against espionage, sabotage, damage and theft.

Priority Intelligence Requirement (PIR)—Those intelligence requirements for which a commander has an anticipated and stated priority in the task of planning and decision-making.

Protection Providing Organization (PPO)—Refers collectively to the U.S. Army Criminal Investigation Command, the Naval Criminal Investigative Service, Air Force Office of Special Investigations, the Defense Criminal Investigative Service, the Pentagon Force Protection Agency and the National Security Agency.

Protective Services—A specialized activity, which increases the personal safety and security of a distinguished visitor or other principal. The activity may be limited to a protective threat assessment or may extend to a major PSO involving considerable manpower and resources.

Protective Service Detail (PSD)—Trained and armed protective security officials capable of providing continuous protection for a designated individual.

RED HORSE—Air Force units are wartime-structured to provide a heavy engineer capability. They have a responsibility across the operational area, are not tied to a specific base, and are not responsible for base operation and maintenance. These units are mobile, rapidly deployable, and largely self-sufficient, for limited periods of time.

Security—For the purposes of this Instruction, measures taken by a military unit, activity, or installation to protect against all acts designed to, or that may, impair its effectiveness. Also, a condition that results from establishing and maintaining protective measures that ensures a state of inviolability from hostile acts or influences.

Self-Supported Separate Facility—A real property entity consisting of one or more of the following: a building, a structure, a utility system, pavement and underlying land that is separate from an installation and has inherent responsibility for emergency response functions, e.g. 911 response functions.

Special Event—An activity characterized by a large concentration of personnel and/or a gathering where distinguished visitors are involved, often associated with a unique or symbolic event.

TACON for FP—TACON that enables the GCC to order implementation of FP measures and to exercise the security responsibilities outlined in any MOA concluded pursuant to MOU between DOS and DOD, "Security of DOD Elements and Personnel in Foreign Areas," (known as the Universal MOU). Further, TACON for FP authorizes the GCC to change, modify, prescribe and enforce FP measures for covered forces. This relationship includes the authority to inspect and assess security requirements, direct DOD activities to identify the resources required to correct deficiencies and submit budget requests to parent organizations to fund identified corrections. The GCC may also direct immediate FP measures (including temporary relocation and departure) when in his or her judgment such measures must be accomplished without delay to ensure the safety of the DOD personnel involved. Persons subject to TACON for FP of a GCC

include Active and Reserve Component personnel (including National Guard personnel in a title 10 status (Sections 134 and 1072(2) of title 10, USC)) in the AOR as well as all DOD civilian employees and their family members in the AOR.

Terrorism—The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. See also antiterrorism; combating terrorism; counterterrorism; force protection condition; terrorist; terrorist groups.

Terrorism Consequence Management—DOD preparedness and response for mitigating the consequences of a terrorist incident, including the terrorist use of WMD. DOD consequence management activities are designed to support the lead Federal agency (domestically, the Department of Homeland Security; foreign, the Department of State) and include measures to alleviate damage, loss of life, hardship, or suffering caused by the incident; protect public health and safety; and restore emergency essential government services.

Terrorism Incident Response Measures—A set of procedures established for response forces to deal with the effects of a terrorist incident.

Terrorism Threat Assessment—The process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat or the product of a threat analysis for a particular unit, installation, or activity.

Terrorism Threat Level (TTL)—An intelligence threat assessment of the level of terrorist threat faced by U.S. personnel and interests. The assessment is based on a continuous intelligence analysis of a minimum of four elements: terrorist group operational capability, intentions, activity and operational environment. There are four threat levels: LOW, MODERATE, SIGNIFICANT and HIGH. Threat levels should not be confused with FPCONs. Threat-level assessments are provided to senior leaders to assist them determining the appropriate local FPCON.

Terrorist—An individual who commits an act or acts of violence or threatens violence in pursuit of political, religious, or ideological objectives.

Terrorist Groups—Any number of terrorists who assemble together, have a unifying relationship, or are organized for the purpose of committing an act or acts of violence or threatens violence in pursuit of their political, religious, or ideological objectives. See also terrorism.

Unit—1. Any military element whose structure is prescribed by competent authority, such as a table of organization and equipment; specifically, part of an organization. 2. An organization title of a subdivision of a group in a task force. 3. With regard to Reserve Components of the Armed Forces, denotes a Selected Reserve unit organized, equipped and trained for mobilization to serve on active duty as a unit or to augment or be augmented by another unit.

Unit Antiterrorism Representative—The principal military or civilian advisor charged with managing the AT program for a unit or DOD element not required to have an ATO as stipulated in AF AT Standard 9.

Vulnerability—In AT, a situation or circumstance which, if left unchanged, may result in the loss of life or damage to mission-essential resources. It includes the characteristics of an installation, system, asset, application, or its dependencies that could cause it to suffer a

degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard.

Vulnerability Assessment (VA)—A Department of Defense, command, or unit-level evaluation (assessment) to determine the vulnerability of a terrorist attack against an installation, unit, exercise, port, ship, residence, facility, or other site. Identifies areas of improvement to withstand, mitigate, or deter acts of violence or terrorism.

Weapons Of Mass Destruction (WMD)—Weapons that are capable of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people. Weapons of mass destruction can be high-yield explosives or nuclear, biological, chemical, or radiological weapons, but exclude the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon.

Attachment 1 (DOVERAFB)

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 10-245, *Air Force Antiterrorism (AT),* 30 March 2009

Prescribed Forms

There are no Prescribed Forms in this publication.

Adopted Forms

AT Form 1, *CVAMP Tracking Sheet*, 1 December 2011

AF Form 2, *Random Antiterrorism Measure Tracking Sheet*, 1 December 2011

Abbreviations and Acronyms

AT – Antiterrorism

AFOSI – Air Force Operations of Special Investigations

BPA - Blanket Purchase Agreement

CAT - Crisis Action Team

CIP - Critical Infrastructure Program

CITA - Commander's Integrated Threat Assessment

DBT - Design Basis Threat

DHS - Department of Homeland Security

EIM - Enterprise Information Management

FPEC - Force Protection Executive Council

FPWG - Force Protection Working Group

IATP - Individual Antiterrorism Terrorism Plan

ICC - Installation Command Center

MANPAD - Man Portable Air Defense

MDG - Medical Group

MEVA - Mission Essential Vulnerable Area

MTT – Mobile Training Team

OPLAN - Operations Plan

PR - Program Review

RA - Risk Assessment

TA - Threat Assessment

TBD – To Be Determined

TIFC - Installation Threat/Intelligence Fusion Cell

TWG – Threat Working Group

Attachment 2

FORCE PROTECTION CONDITION (FPCON) MEASURES

A2.1. General. The DOD FPCON System describes the progressive level of protective measures that are implemented by all the DOD Components in anticipation of or in response to a terrorist threat or attack. The FPCON System is the principal means through which commanders apply an operational decision on how to best guard against the terrorist threat. The protective measures identified in the FPCON System assist commanders in reducing the risks of terrorist attacks and other security threats to DOD personnel, units and activities. The measures below are derived from DOD AT Standard 22 and include AF modifications. Commanders will ensure these measures and developed measures address local and operational risks. Commanders must consider GCC policies, local laws, mutual support agreements and/or the SOFA. Air Force commanders are responsible for implementing FPCON measures.

A2.1.1. Commanders shall ensure the following when implementing FPCON measures:

A2.1.1.1. Ensure there is an effective AT plan and the plan is widely known and practiced in order to use "every airman as a sensor".

A2.1.1.2. Analyze the threat and plan courses of action to defeat those threats. Detailed planning against plausible enemy courses of action will often point to vulnerabilities which can be mitigated through adjustments to TTPs and further mitigated through innovation and programming.

A2.1.1.3. Consider force on force or intruder play to test COAs. Development and implementation of effective friendly COAs to counter known threats offers a reasonable deterrent effect and the opportunity for long-term success against terrorist attack.

A2.1.1.4. Ensure personnel assigned tasks directed by FPCON measures are properly trained and available to carry out the task.

A2.1.1.5. Based on the threat, employ sufficient patrols to deter enemy action, disrupt terrorist planning and respond to incidents or attacks against the installation. Patrols should focus protection on critical operational assets, mission support infrastructure and mass gathering locations.

A2.1.1.6. Consider placing barriers around identified critical assets, facilities with BSAT, restricted areas, high occupancy facilities, flight line entry points and high value resource areas to create standoff.

A2.1.1.7. Review and be familiar with mutual aid and host tenant support agreements. Keep law enforcement agencies (federal, state and local) appraised of the current situation and threat to determine the level of incident support the installation provides or receives.

A2.1.1.8. Ensure the installation Disaster Response Force and its sub elements are trained and available for response as described in AFI 10-2501.

A2.1.2. The DOD FPCON System consists of five progressive levels of increasing AT protective measures.

A2.1.3. Site-specific AT measures and physical security actions, linked to an FPCON, shall be classified "CONFIDENTIAL." When separated from the AT Plan, specific AT measures linked to a FPCON and site-specific FPCON levels may be downgraded to "FOR OFFICIAL USE ONLY," if appropriate.

A2.1.4. Upon declaration of an FPCON level, all listed security measures for that FPCON level shall be implemented immediately unless waived in writing by the appropriate GCC or delegated representative. In non-DOD controlled facilities housing DOD occupants, DOD organizations shall implement applicable FPCON measures in space directly controlled by DOD to the extent possible. The supplementing RAMs and command-unique or site-specific measures should also be implemented to complicate a terrorist group's operational planning and targeting.

A2.1.5. AF installations and separate facilities shall supplement each FPCON measure in this instruction with site-specific details describing how the measure is to be implemented locally, to include responsibilities assigned to subordinate units and organizations.

A2.1.6. Airfield-specific measures are for installations and facilities with a permanently functioning airfield. Installations and facilities with an emergency helicopter pad should review and implement any applicable airfield-specific measures when they anticipate air operations.

A2.1.7. The CBRN related FPCON measures contained in this publication are not all inclusive. Additional CBRN FPCON measures are in the AF Civil Engineer Support Agency (AFCESA) Comprehensive Emergency Management Plan (CEMP) 10-2 template. Each MAJCOM and installation should also develop additional CBRN FPCON measures applicable to their location.

A2.2. FPCON NORMAL. This condition applies when a general global threat of possible terrorist activity exists and warrants a routine security posture. At a minimum, access control will be conducted at all DOD installations and facilities.

A2.2.1. Measure NORMAL 1: Secure and randomly inspect buildings, rooms and storage areas not in regular use.

A2.2.2. Measure NORMAL 2 (AF Modified): Conduct random security checks of vehicles and persons entering facilities under the jurisdiction of the United States.

A2.2.2.1. Measure NORMAL 2.1 (AF Added): Conduct random vehicle inspections at installation entry points in addition to base entry point checks (BEPC) as directed by installation commanders. Implement 100% inspection of large commercial vehicles. MAJCOM and local planners should define large commercial vehicles in integrated defense plans based on geographical location, character of local transport and threat. Conduct random vehicle inspections at entrances to restricted areas beyond inspection requirements listed in AFI 31-101.

A2.2.3. Measure NORMAL 3: Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.

A2.2.4. Measure NORMAL 4 (AF Modified): Identify defense critical infrastructure and critical assets, facilities with BSAT and high occupancy buildings.

A2.2.5. Measure NORMAL 5 (AF Added): Implement a daily RAM program involving the entire installation with emphasis on identifying surveillance activities and disrupting the terrorist attack cycle. Installations will tailor their RAM program to meet the threat and mitigate vulnerabilities.

A2.2.6. Measure NORMAL 6 (AF Added): Conduct 100% identification verification of all vehicle operators and pedestrians entering installations.

A2.2.7. Measure NORMAL 7 (AF Added): Where no permanent channeling measures are built into the gates, emplace barriers or obstacles on in-bound and out-bound lanes at installation entry points to mitigate high-speed installation access through entry and exit lanes, in accordance with UFC 4-022-01. Prevent base entry through exit lanes. Ensure sufficient number and types of barriers remain for increased FPCON/RAMs.

A2.2.8. Measure NORMAL 8 (AF Added): Identify local vendors that are able to provide rapid stocks of emergency response equipment and supplies in accordance with local response plans.

A2.3. FPCON ALPHA. (AF Modified) This condition applies when there is an increased general threat of possible terrorist activity against personnel or facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of FPCON BRAVO measures. However, it may be necessary to implement certain measures from higher FPCONs measures resulting from intelligence received or as a deterrent. The measures in this FPCON must be capable of being maintained indefinitely.

A2.3.1. Measure ALPHA 1: Fully implement all measures of lower FPCON levels.

A2.3.2. Measure ALPHA 2: At regular intervals, inform personnel and family members of the general situation. Ensure personnel arriving for duty are briefed on the threat. Also, remind them to be alert for and to report suspicious activities, such as the presence of unfamiliar personnel and vehicles, suspicious parcels and possible surveillance attempts.

A2.3.2.1. Measure ALPHA 2.1 (AF Added): Post signs at installation gates and utilize mass communication systems to inform/remind personnel of the FPCON level.

A2.3.3. Measure ALPHA 3: The duty officer or personnel with access to building plans as well as the plans for area evacuations must be available at all times. Plans should be in place to execute access control procedures. Key personnel required to implement security plans should be on-call and readily available.

A2.3.4. Measure ALPHA 4 (AF Modified): Increase random security checks of vehicles and persons entering installations or facilities under the jurisdiction of the United States.

A2.3.5. Measure ALPHA 5: Initiate food and water risk management procedures, brief personnel on food and water security procedures and report any unusual activities.

A2.3.6. Measure ALPHA 6 (AF Modified): Test mass notification systems weekly.

A2.3.7. Measure ALPHA 7: Review all plans, identify resource requirements and be prepared to implement measures of the next higher FPCON level.

A2.3.7.1. Measure ALPHA 7.1 (AF added): Review plans (to include AT, Comprehensive Emergency Management Plan, Integrated Defense Plan, Medical Contingency Response Plan/Mass Casualty, Disease Containment Plan, etc.) and most

recent VA reports, and identify resource requirements. Review dependent, civilian and military personnel evacuation plans and support agreements with local officials.

A2.3.8. Measure ALPHA 8 (AF Modified): Review and, if necessary, implement security measures for DOD identified high-risk personnel in accordance with DODI O-2000.22 and AFI 71-101, vol 2, *Protective Service Matters*.

A2.3.9. Measure ALPHA 9 (AF Modified): Consult local authorities on the threat and mutual AT measures. As appropriate, brief law enforcement agencies who provide support to the installation and request assistance as necessary to ensure protection of resources and personnel.

A2.3.10. Measure ALPHA 10: Review intelligence, CI and operations dissemination procedures.

A2.3.11. Measure ALPHA 11: Review barrier plans.

A2.3.12. Measure ALPHA 12 (AF Added): Secure access to all bulk quantity storage areas containing hazardous and flammable material.

A2.3.13. Measure ALPHA 13 (AF Added): Review CBRN detection plan ensuring it uses available detectors (deployment and home station assets).

A2.3.14. Measure ALPHA 14: Review all higher FPCON measures.

A2.4. FPCON BRAVO. Applies when an increased or more predictable threat of terrorist activity exists. Sustaining BRAVO measures for a prolonged period may affect operational capability and military-civil relationships with local authorities.

A2.4.1. Measure BRAVO 1: Fully implement all measures of lower FPCON levels.

A2.4.1.1. Measure BRAVO 1.1 (AF Added): Brief personnel on the updated threat and associated procedures. Update signs at installation gates and utilize mass communication systems to inform/remind personnel of the FPCON level.

A2.4.1.2. Measure BRAVO 1.2 (AF Added): Increase frequency of daily RAMs. Focus additional RAMs on current situation and nature of threat.

A2.4.1.3. Measure BRAVO 1.3 (AF Added): Have intelligence and OSI provide a CBRN threat briefing to the Threat Working Group (TWG) or equivalent. Include specific information such as probability of CBRN use, type(s) and amount of CBRN material, likely CBRN material release mechanisms and probable targets.

A2.4.1.4. Measure BRAVO 1.4 (AF Added): Verify the interoperability of CBRN response procedures with local community resources, to include activities outlined in the CEMP 10-2, Disease Containment Plan (DCP) and Medical Contingency Response Plan (MCRP).

A2.4.1.5. Measure BRAVO 1.5 (AF Added): Contact local hospitals and establish/ensure lines of communication for notification of the installation in the event of significant increase in antibiotic use or people exhibiting symptoms of exposure to CBRN materials.

A2.4.2. Measure BRAVO 2 (AF Modified): Enforce control of entry into facilities containing defense critical infrastructure and critical assets, BSAT, lucrative targets, or high-

profile locations. Randomly search vehicles entering these areas. Particular scrutiny should be given to vehicles that are capable of concealing a large improvised explosive device (IED), e.g., cargo vans or delivery vehicles, sufficient to cause catastrophic damage to property or loss of life.

A2.4.3. Measure BRAVO 3 (AF Modified): Keep cars and objects (e.g., crates, trash containers) away from buildings to reduce vulnerability to bomb attacks. Apply this criterion to all critical and high-occupancy buildings. Consider applying to all inhabited structures to the greatest extent possible. Standoff distance should be determined by the following factors: asset criticality, the protection level provided by structure, IED or Vehicle Borne IED (VBIED) threat and available security measures. Consider centralized parking and implementation of barrier plans. Utilize UFC 4-010-01, *DOD Minimum Antiterrorism Standards for Buildings*, and UFC 4-010-02, *DOD Minimum Antiterrorism Standoff Distances for Buildings.* The AFH 10-2401, *Vehicle Bomb Mitigation Guide*, is an additional tool for standoff planning.

A2.4.4. Measure BRAVO 4: Secure and periodically inspect all buildings, rooms and storage areas not in regular use.

A2.4.5. Measure BRAVO 5: At the beginning and end of each workday, as well as at random intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.

A2.4.6. Measure BRAVO 6: Implement mail-screening procedures to identify suspicious letters and parcels.

A2.4.7. Measure BRAVO 7: Randomly inspect commercial deliveries. Advise family members to check home deliveries.

A2.4.7.1. Measure BRAVO 7.1 (AF Added): Increase random security checks of vehicles and persons entering installations or facilities under the jurisdiction of the United States. Inspect all commercial deliveries (AF Baseline FPCON posture directs inspection of all large commercial vehicles in FPCON Normal).

A2.4.8. Measure BRAVO 8 (AF Modified): Randomly inspect food and water for evidence of tampering or contamination before use by DOD personnel. Inspections should include delivery vehicles, storage areas/facilities and storage containers.

A2.4.9. Measure BRAVO 9: Increase security measures and guard presence or initiate increased patrols and surveillance of DOD housing areas, schools, messes, on-base clubs, military treatment facilities and similar high-occupancy targets to improve deterrence and defense, and to build confidence among staff and family members.

A2.4.10. Measure BRAVO 10: Implement plans to enhance off-installation security for DOD facilities. In areas with Threat Levels of Moderate, Significant, or High, coverage includes facilities (e.g., DOD schools and daycare centers) and transportation services and routes (e.g., bus routes) used by DOD employees and family members.

A2.4.11. Measure BRAVO 11: Inform local security committees of actions being taken.

A2.4.11.1. Measure BRAVO 11.1 (AF Added): Consult local authorities on the threat and mutual AT measures. As appropriate, brief law enforcement agencies who provide support to the installation and request assistance as necessary to ensure protection of

resources and personnel. As appropriate, coordinate with local authorities regarding infrastructure outside the installation, e.g. infrastructure supplying energy to the installation.

A2.4.12. Measure BRAVO 12 (AF Modified): Verify identity of visitors to the installation and randomly inspect their suitcases, parcels and other containers. Visitors are non-DOD affiliated personnel who do not have official DOD credentials authorizing installation access.

A2.4.13. Measure BRAVO 13: Conduct random patrols to check vehicles, people and buildings.

A2.4.14. Measure BRAVO 14: As necessary, implement additional security measures for High-Risk Personnel (HRP).

A2.4.15. Measure BRAVO 15: Place personnel required for implementing AT plans on call; commanders should exercise discretion in approving absences.

A2.4.16. Measure BRAVO 16: Identify and brief personnel who may augment guard forces. Review specific rules of engagement including the use of deadly force.

A2.4.17. Measure BRAVO 17: As deemed appropriate, verify identity of personnel entering buildings.

A2.4.18. Measure BRAVO 18: Review status and adjust as appropriate operations security, communications security and information security procedures.

A2.4.19. Measure BRAVO 19 (AF Modified): (Airfield-specific) Limit access points in order to enforce entry control. As appropriate, erect barriers and establish manned checkpoints at entrances to airfields. Ensure the identity of all individuals entering the airfield (flight line and support facilities) with no exceptions. Randomly inspect vehicles, briefcases and packages entering the airfield.

A2.4.20. Measure BRAVO 20: (Airfield-specific) Coordinate plans to safeguard aircraft departure and approach flight paths with local authorities. Be prepared to activate contingency plans and issue detailed air traffic control procedures. As appropriate, take actions to mitigate the threat of surface- to-air missiles or standoff weapons that can be delivered from beyond the airfield perimeter.

A2.4.21. Measure BRAVO 21 (AF Added): Ensure CBRN detectors are operational as outlined with the detection plan (deployment and home station assets).

A2.4.22. Measure BRAVO 22: Review all higher FPCON measures.

A2.5. FPCON CHARLIE. Applies when an incident occurs or intelligence is received indicating that some form of terrorist action or targeting against personnel or facilities is likely. Prolonged implementation of CHARLIE measures may create hardship and affect the activities of the unit and its personnel.

A2.5.1. Measure CHARLIE 1: Fully implement all measures of lower FPCON levels.

A2.5.1.1. Measure CHARLIE 1.1 (AF Added): Conduct 100% identification checks of all personnel entering the installation, to include vehicle passengers.

A2.5.1.2. Measure CHARLIE 1.2 (AF Added): Brief personnel on the updated threat and associated procedures. Update signs at installation gates and utilize mass communication

systems to inform/remind personnel of the FPCON level. If a CBRN threat exists, ensure the Disaster Response Force and, if permissible, local authorities are briefed on the threat.

A2.5.1.3. Measure CHARLIE 1.3 (AF Added): Increase frequency of daily RAMs. Focus additional RAMs on current situation and nature of threat.

A2.5.2. Measure CHARLIE 2: Recall additional required personnel. Ensure armed augmentation security personnel are aware of current rules of engagement and any applicable Status of Forces Agreements (SOFA). Review types of weapons and ammunition issued to augmentation security personnel; heightened threats may require employment of different weapon capabilities.

A2.5.3. Measure CHARLIE 3: Be prepared to react to requests for assistance from both local authorities and other installations in the region.

A2.5.3.1. Measure CHARLIE 3.1 (AF Added): Ensure flow of information between on and off-base medical treatment facilities participating in the medical surveillance program. Consider initiation of manual collection of data if the automated system has a 24-hour or more delay in providing results.

A2.5.3.2. Measure CHARLIE 3.2 (AF Added): Consider Noncombatant Evacuation Operations (NEO).

A2.5.4. Measure CHARLIE 4: Limit access points in order to enforce entry control. Randomly search vehicles.

A2.5.4.1. Measure CHARLIE 4.1 (AF Added): Increase random security checks of vehicles and persons entering installations or facilities under the jurisdiction of the United States.

A2.5.4.2. Measure CHARLIE 4.2 (AF Added): Implement procedures to expedite the entry of first and emergency responders onto the installation during emergencies. Ensure these procedures prevent unauthorized entry.

A2.5.5. Measure CHARLIE 5: Ensure or verify the identity of all individuals entering food and water storage and distribution centers use sign-in and sign-out logs at access control and entry points, and limit or inspect all personal items.

A2.5.6. Measure CHARLIE 6 (AF Modified): Initiate contingency (credible CBRN threat) monitoring for chemical, biological and radiological contamination as required. Suspend contractors and off-facility users from tapping into the facility water system. An alternate locally developed measure should be implemented when contractors are responsible for DOD water supplies or when water is provided by local (non-DOD) sources or agencies.

A2.5.6.1. Measure CHARLIE 6.1 (AF Added): If a CBRN threat exists, ensure all shortages of CBRN equipment and its potential impact is briefed to the installation commander.

A2.5.6.2. Measure CHARLIE 6.2 (AF Added): Verify operation, deploy and begin using all available CBRN detectors (deployment and home station) as outlined in the detection plan.

A2.5.7. Measure CHARLIE 7: Increase standoff from sensitive buildings based on the threat. Implement barrier plan to hinder vehicle-borne attack.

A2.5.8. Measure CHARLIE 8 (AF Modified): Increase patrolling of the installation/facility to include waterside perimeters, if appropriate. Be prepared to assist local authorities in searching for threatening actions/persons outside the facility perimeter. For airfields, patrol or provide observation of aircraft parking areas and approach and departure flight corridors as appropriate to the threat (coordinate with Transportation Security Administration, Marine Patrol, United States Coast Guard and local law enforcement as required to cover off-facility approach and departure flight corridors).

A2.5.9. Measure CHARLIE 9 (AF Modified): Increase protection for all defense critical infrastructure, critical assets or BSAT facilities. Give special attention to and coordinate with local authorities regarding infrastructure outside the military establishment.

A2.5.9.1. Measure CHARLIE 9.1 (AF Added): Consider closing or enhancing security at remote sites and alternate, practice or training airfields.

A2.5.9.2. Measure CHARLIE 9.2 (AF Added): Protect DOD personnel at vulnerable mass gathering facilities during peak usage, especially near the installation perimeter. Coordinate protection of mass gathering facilities off the installation with civilian law enforcement agencies.

A2.5.10. Measure CHARLIE 10: To reduce vulnerability to attack, consult local authorities about closing public (and military) roads and facilities and coordinate any other precautionary measures taken outside the installation perimeter.

A2.5.11. Measure CHARLIE 11: Randomly inspect suitcases, briefcases and packages being brought onto the installation through access control points and consider randomly searching them upon leaving the installation.

A2.5.12. Measure CHARLIE 12: Review personnel policy procedures to determine appropriate courses of action for dependent family members.

A2.5.13. Measure CHARLIE 13: Review access procedures for all non-U.S. personnel and adjust as appropriate. For airfields, consider terminating visitor access to the flight line and support facilities.

A2.5.14. Measure CHARLIE 14: Consider escorting children to and from DOD schools (among options to consider are escorting school buses, recommending parents escort children to/from school, etc.).

A2.5.15. Measure CHARLIE 15: (Airfield-specific) Reduce flying to only essential operational flights. Implement appropriate flying countermeasures as directed by the Flight Wing Commander (military aircraft) or Transportation Security Administration (civilian aircraft). Consider relief landing ground actions to take for aircraft diversions into and out of an attacked airfield. Consider augmenting fire-fighting details.

A2.5.15.1. Measure CHARLIE 15.1 (AF Added): Consider aircraft dispersal, or the dispersal of other high value assets, based on assessment of local threat from standoff weapons, vulnerability of the assets and operational feasibility.

A2.5.16. Measure CHARLIE 16: Review all FPCON DELTA measures.

A2.6. FPCON DELTA. Applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is

imminent. FPCON DELTA is usually declared as a localized condition. FPCON DELTA measures are not intended to be sustained for an extended duration.

A2.6.1. Measure DELTA 1 (AF Modified): Fully implement all measures of lower FPCON levels. As necessary, brief personnel on the updated threat and associated procedures and update signs at installation gates, utilize mass communication systems to inform/remind personnel of the FPCON level.

A2.6.2. Measure DELTA 2: Augment guards as necessary.

A2.6.3. Measure DELTA 3: Identify all vehicles within operational or mission support areas.

A2.6.4. Measure DELTA 4: Search all vehicles and their contents before allowing entrance to the installation. Selected pre-screened and constantly secured vehicles used to transport escorted very important personnel may be exempted.

A2.6.5. Measure DELTA 5: Control facility access and implement positive identification of all personnel with no exceptions.

A2.6.6. Measure DELTA 6: Search all personally carried items (e.g., suitcases, briefcases, packages, backpacks) brought into the installation or facility.

A2.6.7. Measure DELTA 7: Close DOD schools.

A2.6.8. Measure DELTA 8: Make frequent checks of the exterior of buildings and of parking areas.

A2.6.9. Measure DELTA 9: Restrict all non-essential movement.

A2.6.10. Measure DELTA 10: (Airfield specific) Cease all flying except for specifically authorized operational sorties. Be prepared to deploy light aircraft and/or helicopters for surveillance tasks or to move internal security forces. Implement, if necessary, appropriate flying countermeasures.

A2.6.11. Measure DELTA 11: (Airfield specific) As appropriate, airfields should prepare to accept aircraft diverted from other stations.

A2.6.12. Measure DELTA 12: If permitted, close public and military roads and facilities. If applicable, close military roads allowing access to the airfield.

A2.6.13. Measure DELTA 13: Begin continuous monitoring for chemical, biological and radiological contamination.

A2.6.14. Measure DELTA 14 (AF Added): If not already accomplished and a credible threat exists, initiate collective protection operations, as explained in AFMAN 10-2602, *Nuclear, Biological, Chemical, and Conventional (NBCC) Defense Operations and Standards*.

Attachment 3

TERRORIST THREAT LEVELS

A3.1. General. The standardized DOD methodology that describes the terrorist threat to DOD personnel, facilities and interests shall be used to determine Terrorism Threat Levels (TTL). The Defense Intelligence Agency (DIA) sets the DOD TTL for all countries. Terrorism threat levels are established as the result of all-source analysis and incorporation of GCC and Military Department input. The JITF-CT coordinates country TTLs with appropriate GCCs, Services and Defense Attaches.

A3.1.1. DIA and the responsible GCC may assign different threat levels to the same country. This is possible because analysts occasionally disagree about the conclusions to be drawn from available information. Threat assessments provide information to assist commanders in determining the appropriate FPCON level and measures. FPCON level declarations remain the exclusive responsibility of commanders. Threat levels are not tied to FPCON levels in any way and should not be confused. National-level DOD organizations cannot provide all intelligence that might be needed to make FPCON level determinations. Information from regional and tactical intelligence and local law enforcement authorities must also be considered.

A3.1.2. Threat assessments are not to be confused with DOD-designated high physical threat countries. DOD-designated high physical threat countries pertain exclusively to the DOD Travel Security Policy.

A3.2. Terrorist Threat Levels. In assessing the terrorist threat to U.S. personnel and interests, DOD intelligence agencies use a four-step scale to describe the severity of the threat. The following lists the threat levels and the combinations of analysis-based factors used to determine the level:

A3.2.1. **HIGH:** Anti-US terrorists are operationally active and use large casualty-producing attacks as their preferred method of operation. There is a substantial DOD presence and the operating environment favors the terrorist.

A3.2.2. **SIGNIFICANT:** Anti-US terrorists are present and attack personnel as their preferred method of operation or a group uses large casualty producing attacks as their preferred method, but has limited operational activity. The operating environment is neutral.

A3.2.3. **MODERATE:** Terrorists are present, but there are no indications of anti-US activity. The operating environment favors the Host Nation/US.

A3.2.4. **LOW:** No group is detected or the group activity is non-threatening.

A3.3. Terrorist threat levels are a product of the following four factors.

A3.3.1. **Operational Capability**. This factor focuses on the attack methods used by the group and other measures that enhance its effectiveness, such as state sponsorship and ingenious use of technology. The key element is whether the group has the capability and willingness to conduct large casualty producing attacks, for example a suicide vehicle bomb containing thousand of kilograms of explosives or WMD timed to kill the most personnel at the target. Groups that selectively assassinate individuals or conduct late night bombings

causing limited property damage pose a decreasing threat. The ability to operate on a regional or transnational basis and the overall professionalism of the group is also assessed.

A3.3.2. **Intentions**. This factor is the stated desire or history of terrorist attacks against U.S. interests. Recent substantial attacks in the country or, if the group is transnational, the conduct of operations in other countries is the higher end of the threat scale. This is especially true if the intentions are anti-DOD. The basis of the group ideology, whether the group is more focused on the host nation rather than U.S. interests is the other key component. Whether the group will react to high profile U.S. led international events, such as intervention in the Balkans, is also considered and rated.

A3.3.3. **Activity**. This factor is an assessment of the actions the group is conducting and whether that activity is focused on serious preparations for an attack. The highest threat is credible indications of U.S. targeting to include the movement of key operatives, final intelligence collection and movement of weapons to the target vicinity. Less threatening actions are contingency planning, training and logistical support. Activities that would make the group less likely to attack, such as robust fund raising or effective safe haven are considered. Whether the group has recently been disrupted by arrests or strikes on training camps will reduce the threat, at least in the short term.

A3.3.4. **Operating Environment**. This factor rates how the overall environment influences the ability, opportunity and motivation to attack DOD interests in a given location. An important element of this factor is the capability of the host nation security apparatus to combat terrorism, its degree of cooperation with the U.S. and the quality of the reporting on terrorist groups in the country. A key element is whether there is a DOD presence and if so the type, size, location, political sensitivity and if temporary, its duration. It is also important to consider if the group is focused on DOD as its primary target for anti-US attacks. Another part of this factor is the overall political, economic and military stability of the country and its effect on the ability of a group to attack.

Attachment 4

RISK MANAGEMENT AND RESOURCING PROCESSES

A4.1. Overview. The commander has an inherent command responsibility to reduce risks that threaten the mission with available resources. Risk management described in AFPD 31-1, aids the commander in assessing risk. If the commander cannot internally correct, mitigate or assume risk, they must elevate these vulnerabilities and associated risk(s) through CVAMP. CVAMP will forward the vulnerability through the chain of command to the GCC, who will decide if the vulnerability will be reported higher.

A4.2. Resourcing. Emphasis should be placed on acquiring resources to detect, assess, warn, defend or recover in order to prevent hostile acts or mitigate the effects. It is inherent upon the organization to assess the resource requirement against other organizational unfunded or funded requirements and determine if an internal reallocation of funding is appropriate and possible. CVAMP is used to collate and track AT vulnerabilities and resourcing. The status of vulnerabilities entered into CVAMP should be documented in CVAMP.

A4.3. AF Funding Sources.

A4.3.1. Planning, Programming, Budget and Execution (PPB&E). The PPB&E process includes requests considered during the POM funding cycle. This program is for long term planning and the funds will not be available for two to five years. Information on the PPB&E process can be found in the DOD Management Initiative Decision 913.

A4.3.2. Installation and MAJCOM budget process and commander's discretionary funds.

A4.3.3. Many PEC and/or funding appropriations (AT, Physical Security, EM, Medical, Construction, Base Defense, Base Operating Support, Communications, Weapons of Mass Destruction Threat Response; Nuclear, Biological and Chemical Defense Program; Fire Emergency Services; Sustainment Restoration and Modernization (SRM) and military construction (MILCON), etc.) may be used to fund AT resourcing activities. Commanders will consider all PEC and Funding Appropriation sources as authorized by law and AF policy and guidance.

A4.3.4. Use Antiterrorism Program Element 28047F as the primary funding source for manpower authorizations, antiterrorism equipment, procurement, military construction and the associated costs specifically identified and measurable to those resources and activities associated with the Air Force AT Program.

A4.3.5. Specialized funds designed for AT and the war on terrorism.

A4.4. Combating Terrorism Readiness Initiative Fund (CbT-RIF). This program was established by Congress and is managed by the Joint Staff (J-3). It provides funds for emergency or unforeseen (emergent) high priority force protection projects or equipment. It is designed for requirements that need to be funded in the current fiscal year and provides a means for the GCC to react to unforeseen requirements from changes in a terrorist threat, threat levels, force protection doctrine/standards, as well as unanticipated requirements identified as a result of VAs, tactical operations and exercising AT Plans. If maintenance funds for CbT-RIF projects are not programmed and provided from the parent Service, CbT-RIF can be used to fund maintenance costs for those CbT-RIF-funded items during the year of purchase and the subsequent year as a

temporary measure to permit the Service adequate time to program life-cycle costs. The fund is not intended to subsidize ongoing projects, supplement budget shortfalls, or support routine activities, which are a Service responsibility. Requests must be submitted through the responsible MAJCOM and GCC, per GCC policies, to the Joint Staff. Submission instructions are outlined in CJCSI 5261.01E, *Combating Terrorism Readiness Initiatives Fund.*

A4.4.1. **Emergency CbT-RIF Requirement.** An unanticipated requirement created by a combination of circumstances or the resulting state that requires immediate action to prevent, deter, or respond to a terrorist act.

A4.4.2. **Emergent CbT-RIF Requirement.** A newly formed, unexpected requirement resulting from a logical consequence of unforeseen circumstances calling for prompt action.

A4.4.3. GCCs must submit requests for CbT-RIF funds through CVAMP.

A4.4.4. Emergent requirements should be less than 2 years old. The requestor must have an approved, executable and exercised AT Plan.

A4.5. Effectively Managing the Resource Allocation Process.

A4.5.1. Ensure you plan for training and maintenance costs into the out years.

A4.5.2. The ATO needs to work closely with affected functional areas, installation financial advisors/comptroller and contracting from the beginning to address requirements. This will assist in identifying the appropriation sources and funding amounts.

A4.5.3. Adequately articulating and justifying requirements is crucial.

A4.5.4. Determine all appropriate potential funding sources and submit requests through the various channels. Once a requirement is funded by a source, cancel the other requests. **Note**: The Joint Staff does not allow the same request to be submitted through both the PPB&E and CbT-RIF process.

A4.5.5. There are organizations that can aid the commander in identifying technology to satisfy requirements: Physical Security Equipment Action Group (PSEAG), Technical Support Working Group (TSWG), AFSFC Concepts Division, Joint Requirement Office for Chemical, Biological, Radiological and Nuclear Defense (JRO-CBRND) and the Joint Non-Lethal Weapons Directorate (JNLWD). These organizations are separately funded to provide COTS information, rapid prototyping and research and development and/or evaluation of solutions for units in the field. They can provide information and research on technology and equipment evaluated and deemed suitable for your purpose. Additionally, they can provide field assessments to assist in identifying the optimal solutions to meet your requirements.

Attachment 5

AF APPROVED LEVEL II - ATO TRAINING SCHOOLS

A5.1. Attending any of the following schools may certify AF personnel for completion of Level II - ATO Training.

Table A5.1. Air Force Level II - ATO Training.

Air Combat Command 99th Security Forces Group Nellis AFB , NV Phone: DSN 682-1603
United States Air Force Expeditionary Center Ft Dix, NJ Phone: DSN 944-4101 (ext 185)
United States Air Force Special Operations School Hurlburt Field, FL Phone: DSN 579-6330
Air Force Reserve Command 610th Security Forces Squadron Conducts Mobile Training Team (MTT) courses Naval AS, Ft Worth TX Phone: DSN 739-5101 (ext 141, 134, 127)
US Air Forces in Europe Ramstein AB, GE Phone: DSN 314 480-6006
90th Ground Tactical Training Squadron F.E. Warren AFB, WY Phone: DSN 481-7629
96 Ground Combat Training Squadron (GCTS) Eglin AFB, FL Conducts MTT courses Phone: DSN 872-6172
PACAF Regional Training Center

736 SFS/Commando Warrior Andersen AB GU Phone: DSN 315 366-6087
PACAF ANSER MTT 25 E. Street Suite M-307 Hickam AFB, HI Phone: DSN 315 448-2481

Attachment 6 (Added-DOVERAFB)

DEMOGRAPHY/MISSION, SYMBOLISM, HISTORY, ACCESSIBILITY, RECOGNIZIBILITY, POPULATION AND PROXIMITY (DSHARPP OR MSHARPP)

MATRIX EXPLANATION

A6.1. The purpose of the D(M)SHARPP matrix is to analyze likely terrorist targets. Consideration is given to the local threat, likely means of attack available to the enemy, and variables affecting the disposition (e.g., "attractiveness" to enemy, potential psychological effect on community, etc.) of potential targets. This document provides an example of how to use D(M)SHARPP.

A6.1.1. After developing a list of potential targets, use the D(M)SHARPP selection factors to assist in further refining your assessment by determining the most likely (i.e., efficient, effective, and plausible) method of attack and identifying vulnerabilities to that type of attack. After the D(M)SHARPP values for each target or component are assigned, the sum of the values indicate the highest value target (for a particular mode of attack) within the limits of the enemy's known capabilities.

A6.2. DEMOGRAPHY.

A6.2.1. Demography focuses mainly on the threat to personnel and asks the question "who are the targets?" Depending on the ideology of the terrorist group(s), being a member of a particular demographic group can make someone (or some group) a more likely target. Therefore, when assessing points in this area, determine whether or not the group(s) have a history of or are predicted to target:

A6.2.1.1. Military members.

A6.2.1.2. Family members (US citizens in general).

A6.2.1.3. Civilian employees of the US government (include local nationals).

A6.2.1.4. Senior officers or other high-risk personnel.

A6.2.2. Assess points to the target facility (scale of *1-5; 5* being worst) in this area based upon the MO of the group in targeting specific groups, and the potential for the target to be attacked based on its housing personnel of that particular group.

A6.2.3. Demography Criteria Scale:

A6.2.3.1. Facility routinely contains substantial numbers of personnel known to be targeted by the enemy.

A6.2.3.2. Contains known target group, but rarely in large concentrations.

A6.2.3.3. Little target value based on demographics of occupants.

A6.3. MISSION.

A6.3.1. Mission focuses mainly on the threat to the situations, activities, capabilities, and resources on an installation that are vulnerable to a terrorist attack. The mission components consist of the equipment, information, facilities, and/or operations or activities that are necessary to accomplish the installation's mission. When assessing points in this area,

determine whether or not an attack on mission components will cause degradation by assessing the components:

A6.3.1.1. Importance: Importance measures the value of the area or assets located in the area, considering their function, inherent nature, and monetary value.

A6.3.1.2. Effect: Effect measures the ramifications of a terrorist incident in the area, considering the psychological, economic, sociological, and military impacts.

A6.3.1.3. Recoverability: Recoverability measures the time required for the function occurring at that area to be restored, considering the availability of resources, parts, expertise and manpower, and redundancies.

A6.3.2. Assess points to the target equipment, information, facilities, and/or operations or activities (scale of 1-5; 5 being worst) in this area based upon the degree of mission degradation if attacked by a terrorist.

A6.3.3. Mission Criteria Scale:

A6.3.3.1. Installation cannot continue to carry out its mission until the attacked asset is restored.

A6.3.3.2. Ability to carry out a primary mission of the installation would be significantly impaired if this asset were successfully attacked.

A6.3.3.3. Half of the mission capability remains if the asset were successfully attacked.

A6.3.3.4. The installation could continue to carry out its mission if this asset were attacked, albeit with some degradation in effectiveness.

A6.3.3.5. Destroying or disrupting this asset would have no effect on the ability of the installation to accomplish its mission.

A6.4. SYMBOLISM.

A6.4.1. A consider whether the target represents, or is perceived by the enemy to represent, a symbol of a targeted group (e.g., symbolic of US military, Christianity, government, authority, etc.). Assess points in this area based upon the symbolic value of the target to the enemy.

A6.4.2. Symbolism Criteria Scale:

A6.4.2.1. High profile, direct symbol of target group or ideology.

A6.4.2.2. Low profile, direct symbol of target group or ideology.

A6.4.2.3. Low profile and/or obscure symbol of target group or ideology.

A6.4.2.4. **(For MISSION)** Asset is perceived to be vital to the mission of the installation.

A6.5. HISTORY.

A6.5.1. Do terrorist groups have a history of attacking this type of target? While you must consider terrorist trends worldwide, focus on local targeting history and capabilities.

A6.5.2. History Criteria Scale:

A6.5.2.1. Strong history of attacking this type of target.

A6.5.2.2. History of attacking this type of target, but none in the immediate past.

A6.5.2.3. Little to no history of attacking this type of target.

A6.6. ACCESSIBILITY.

A6.6.1. A target is accessible when an operational element can reach the target with sufficient personnel and equipment to accomplish its mission. A target can be accessible even if it requires the assistance of knowledgeable insiders. This assessment entails identifying and studying critical paths that the operational element must take to achieve its objectives, and measuring those things that aid or impede access. The enemy must not only be able to reach the target but must also remain there for an extended period. The four basic stages to consider, when assessing accessibility are:

A6.6.1.1. Infiltration from the staging base to the target area.

A6.6.1.2. Movement from the point of entry to the target or objective.

A6.6.1.3. Movement to the target's critical element.

A6.6.1.4. Exfiltration.

A6.6.2. Accessibility Criteria Scale:

A6.6.2.1. Easily accessible, standoff weapons can be employed.

A6.6.2.2. Inside Perimeter fence, climbing or lowering required.

A6.6.2.3. Not accessible or inaccessible without extreme difficulty.

A6.7. RECOGNIZABILITY.

A6.7.1. A target's recognizability is the degree to which an operational element and/or intelligence collection and reconnaissance asset under varying conditions can recognize it. Weather has an obvious and significant impact on visibility (yours and the enemy's). Rain, snow, and ground fog may obscure observation. Road segments with sparse vegetation and adjacent high ground provide excellent conditions for good observation. Distance, light, and season must be considered.

A6.7.2. Other factors that influence recognizability include the size and complexity of the target, the existence of distinctive target signatures, the presence of masking or camouflage, and the technical sophistication and training of the enemy.

A6.7.3. Recognizability Criteria Scale:

A6.7.3.1. Target is clearly recognizable under all conditions and from a distance; requires little or no training for recognition.

A6.7.3.2. Target is easily recognizable at small-arms range and requires a small amount of training for recognition.

A6.7.3.3. Target is difficult to recognize at night or in bad weather, or might be confused with other targets; requires training for recognition.

A6.7.3.4. Target cannot be recognized under any conditions—except by experts.

A6.8. POPULATION.

A6.8.1. What is the population relative to other potential targets? Going on the assumption the intent of the attack is to kill or injure personnel, it follows that the more densely populated an area/facility is, the more lucrative a target it makes (all other things being equal).

A6.8.2. Population Criteria Scale:

A6.8.2.1. Densely populated; prone to frequent crowds.

A6.8.2.2. Relatively large numbers of people, but not in close proximity (i.e., spread out and hard to reach in a single attack).

A6.8.2.3. Sparsely populated; prone to having small groups or individuals.

A6.8.2.4. **(For MISSION)** The population is comprised of personnel deemed vital to the accomplishment of the installation's mission.

A6.8.2.5. **(For MISSION)** Population has no special segment necessary for mission accomplishment.

A6.8.2.6. **(For MISSION)** Sparsely populated or unattended.

A6.9. PROXIMITY.

A6.9.1. Is the potential target located near other personnel, facilities, or resources that, because of their intrinsic value or "protected" status and a fear of collateral damage, afford it some form of protection? (i.e., near national monuments, protected/religious symbols, etc., which the enemy holds in high regard). *NOTE:* It is important to consider whether the target is in close proximity to other likely targets. Just as the risk of unwanted collateral damage may decrease the chances of attack; a "target-rich" environment may increase the chances of attack.

A6.9.2. Proximity Criteria Scale:

A6.9.2.1. Target is isolated; no chance of unwanted collateral damage to protected symbols or personnel.

A6.9.2.2. Target is in close enough proximity to place protected personnel, facilities, etc., at risk of injury or damage, but not destruction.

A6.9.2.3. Target is in close proximity; serious injury/damage or death/total destruction of protected personnel/facilities likely.

A6.9.3. **Table A6.1** is an example DSHARPP worksheet. **Table A5.2** is an example MSHARPP worksheet. Values from 1 to 5 are assigned to each factor based on the associated data for each target. Five represents the highest vulnerability or likelihood of attack and I the lowest. Accordingly, the higher the total score, the more vulnerable the target. Because this analysis is highly subjective, some analysts prefer simple 'stoplight' charts with red, yellow and green markers representing descending degrees of vulnerability. The D(M)SHARPP analysis must consider both the present force protection posture and enhanced postures proposed for escalating FPCONs.

Table A6.1. DSHARPP Worksheet.

TARGET	D	S	H	A	R	P	P	TOTAL	WEAPON
Barracks A	4	4	5	1	3	3	1	21	4000 lb. Truck IED
Barracks B	4	4	5	4	2	5	4	28	4000 lb. Truck IED
HQ Bldg	5	5	4	1	4	3	2	24	50 lb. Satchel Charge
Pax Terminal	3	3	3	2	3	1	5	20	220 lb. Car IED
BX	2	2	1	3	4	2	3	17	4000 lb. Truck IED
Family Housing		1	2	5	1	4	1	15	220 lb. Car IED
Parade Ground	5	2	4	5	5	5	3	29	Small Unit Raid

Table A6.2. MSHARPP Worksheet.

TARGET	M	S	H	A	R	P	P	TOTAL	WEAPON
HQ Bldg	3	4	5	1	3	3	1	20	4000 lb. Truck IED
Barracks B	3	4	5	4	4	4	2	26	220 lb. Car IED
Comm Center	5	4	2	3	5	2	1	23	4000 lb. Truck IED
SF Ops Center	3	3	2	4	4	4	2	22	7.62 (Sniper)
Fuel Storage	4	3	*1*	*5*	*5*	*1*	3	22	50 lb. Satchel Charge
Hanger A	5	5	3	2	5	5	4	29	Mortar
Weapons Storage	*5*	*5*	*1*	1	*5*	3	1	21	RPG
Electric Transformer	5	2	3	5	5	1	4	25	Grenade

A6.9.4. Specific target vulnerabilities must be combined with exploitable perimeter control vulnerabilities. If access routes are well protected and not deemed exploitable an otherwise vulnerable building becomes a less likely target.

Attachment 7 (Added-DOVERAFB)

CARVER TARGET ANALYSIS TOOL

A7.1. The following is an explanation of the CARVER targeting process. US Special Operations Forces (SOF) uses this process in targeting adversary's installations. For that reason it is included as a tool to evaluate US installations from an adversarial point of view. For those familiar with the CARVER tool, it may be used in addition to or in lieu of other assessment processes.

A7.2. TARGET ANALYSIS PROCESS

A7.2.1. This attachment explains CARVER. CARVER is used to assess mission, validity, and requirements. It is also used in technical appreciation and target analysis. This attachment provides a step-by-step example of how to use CARVER.

A7.3. CRITICALITY, ACCESSIBILITY, RECUPERABILITY, VULNERABILITY, EFFECT, AND RECOGNIZABILITY FACTORS

A7.3.1. The CARVER selection factors assist in selecting the best targets or components to attack. As the factors are considered, they are given a numerical value. This value represents the desirability of attacking the target. The values are then placed in a decision matrix. After CARVER values for each target or component are assigned, the sum of the values indicate the highest value target or component to be attacked within the limits of the statement of requirements and commander's intent.

A7.4. CRITICALITY

A7.4.1. Criticality means target value. This is the primary consideration in targeting. A target is critical when its destruction or damage has a significant impact on military, political, or economic operations.

A7.4.2. Targets within a system must be considered in relation to other elements of the target system. The value of a target will change as the situation develops, requiring the use of time-sensitive methods respond to changing situations. For example, when one has few locomotives, railroad bridging may be less critical as targets; however, safeguarding bridges may be critical to maneuvering conventional forces that require use of such bridges. Criticality depends on several factors:

A7.4.2.1. Time: How rapidly will the impact of the target attack affect operations?

A7.4.2.2. Quality: What percentage of output, production, or service will be curtailed by target damage?

A7.4.2.3. Surrogates: What will be the effect on the output, production, and service?

A7.4.2.4. Relativity: How many targets are there? What are their positions? How is their relative value determined? What will be affected in the system or complex "stream"?

A7.4.3. **Table A7.1** shows how criticality values are assigned on CARVER matrixes.

Table A7.1. Assigning Criticality Values.

CRITERIA	SCALE
Immediate halt in output, production, or service; target cannot function without it.	9-10
Halt within 1 day, or 66% curtailment in output, production, or service	7-8
Halt within 1 week, or 33% curtailment in output, production, or service	5-6
Halt within 10 days, or 10% curtailment in output, production, or service	3-4
No significant effect on output, production or service	1-2

A7.5. ACCESSIBILITY

A7.5.1. A target is accessible when an operational element can reach the target with sufficient personnel and equipment to accomplish its mission. A target can be accessible even if it requires the assistance of knowledgeable insiders. This assessment entails identifying and studying critical paths that the operational element must take to achieve its objectives, and measuring those things that aid or impede access. The adversary must not only be able to reach the target but must also remain there for an extended period. The four basic steps identifying accessibility are:

A7.5.1.1. Infiltration from the staging base to the target area.

A7.5.1.2. Movement from the point of entry to the target or objective.

A7.5.1.3. Movement to the target's critical element.

A7.5.1.4. Exfiltration.

A7.5.2. Factors considered when evaluating accessibility include, but are not limited to:

A7.5.2.1. Active and passive early warning systems.

A7.5.2.2. Swimmer detection devices.

A7.5.2.3. Air defense capabilities within the target area.

A7.5.2.4. Road and rail transportation systems.

A7.5.2.5. Type of terrain and its use.

A7.5.2.6. Concealment and cover.

A7.5.2.7. Population density.

A7.5.2.8. Other natural or synthetic obstacles and barriers.

A7.5.2.9. Current and climatic weather conditions.

A7.5.3. The analysis along each critical path to the target should measure the time it would take for the action element to bypass, neutralize, or penetrate barriers and obstacles along the way. Accessibility is measured in terms of relative ease or difficulty of movement for the operational element and the likelihood of detection. The use of standoff weapons should always be considered in such evaluations.

A7.5.4. **Table A7.2** shows how accessibility values are assigned on CARVER matrices.

Table A7.2. Assigning Accessibility Values.

CRITERIA	SCALE
Easily accessible, standoff weapons can be employed	9-10
Inside a perimeter fence but outdoors	7-8
Inside a building but on ground floor	5-6
Inside a building but on second floor or in basement; climbing or lowering required	3-4
Not accessible or inaccessible without extreme difficulty	1-2

A7.6. RECUPERABILITY

A7.6.1. A target's recuperability is measured in time; that is, how long will it take to replace, repair, or bypass the destruction of or damage to the target? Recuperability varies with the sources and type of targeted components and the availability of spare parts availability. Factors which should be considered when assessing recuperability include, but are not limited to, the availability of:

A7.6.1.1. On-hand equipment such as railroad cranes, dry docks, and cannibalization.

A7.6.1.2. Restoration and substitution through redundancies.

A7.6.1.3. On hand spares.

A7.6.1.4. Equivalent OB equipment sets that backup critical equipment or components, and effects of economic embargoes and labor unrest.

A7.6.2. **Table A7.3** shows how recuperability values are assigned on CARVER matrices.

Table A7.3. Assigning Recuperability Values.

CRITERIA	SCALE
Replacement, repair, or substitution requires 1 month or more	9-10
Replacement, repair, or substitution requires 1 week to 1 month	7-8
Replacement, repair, or substitution requires 72 hours to 1 week	5-6
Replacement, repair, or substitution requires 24 to 72	3-4

hours	
Same day replacement, repair, or substitution	1-2

A7.7. VULNERABILITY

A7.7.1. A target is vulnerable if the adversary has the means and expertise to successfully attack the target. When determining the vulnerability of a target, the scale of the critical component needs to be compared with the capability of the attacking element to destroy or damage it. In general, the attacking element may tend to:

A7.7.1.1. Choose special components.

A7.7.1.2. Do permanent damage.

A7.7.1.3. Prevent or inhibit cannibalization.

A7.7.1.4. Maximize effects through the use of onsite materials.

A7.7.1.5. Cause the target to self-destruct.

A7.7.2. Specifically, vulnerability depends on:

A7.7.2.1. The nature and construction of the target.

A7.7.2.2. The amount of damage required.

A7.7.2.3. The assets available; for example, personnel, expertise, motivation, weapons, explosives, and equipment.

A7.7.3. **Table A7.4** shows how vulnerability values are assigned on CARVER matrices.

Table A7.4. Assigning Vulnerability Values.

CRITERIA	SCALE
Vulnerable to long-range laser target designation, small arms fire, or charges of 5 pounds or less	9-10
Vulnerable to light anti-armor weapons fire or charges of 5 to 10 pounds	7-8
Vulnerable to medium anti-armor weapons fire, bulk charges of 10 to 30 pounds, or very careful placement of smaller charges	5-6
Vulnerable to heavy anti-armor fire, bulk charges of 30 to 50 pounds, or requires special weapons	3-4
Invulnerable to all but the most extreme targeting measures	1-2

A7.8. EFFECT.

A7.8.1. The effect of a target attack is a measure of possible military, political, economic, psychological, and sociological impacts at the target and beyond. This is closely related to the measure of target criticality. The type and magnitude of given effects desired will help

the adversary select targets and target components for attack. Effect in this context addresses all significant effects, whether desired or not, that may result once the selected target component is attacked. Traditionally, this element has addressed the effect on the local population, but now there are broader considerations. Effect is frequently neutral at the tactical adversarial level. For example, the primary effect of the destruction of two adjacent long-range radar sites in an early warning system may be to open a hole in the system that is of sufficient size and duration to permit our adversary to launch a successful attack against the installation. Effects can also include:

A7.8.1.1. The triggering of countermeasures.

A7.8.1.2. Support or negation of PSYOP themes.

A7.8.1.3. Unemployment.

A7.8.1.4. Reprisals against the civilian populace.

A7.8.1.5. Collateral damage to other targets.

A7.8.2. Possible effects can be speculative and should be labeled as such. Effects of the same attack may be quite different at the tactical, operational, and strategic levels. For example, the destruction of a substation may not affect local power supply but cuts off all power to an adjacent region.

A7.8.3. **Table A7.5** shows how effect values are assigned on CARVER matrices.

Table A7.5. Assigning Effect Values.

CRITERIA	SCALE
Overwhelmingly positive effects; no significant negative effects	9-10
Moderately positive effects; few significant negative effects	7-8
No significant effects, neutral	5-6
Moderately negative effects, few significant positive effects	3-4
Overwhelmingly negative effects; no significant positive effects	1-2

A7.9. RECOGNIZABILITY

A7.9.1. A target's recognizability is the degree to which it can be recognized by the adversary and his intelligence collection and reconnaissance assets, under varying conditions. Weather has an obvious and significant impact on visibility. Rain, snow, and ground fog may obscure observation. Road segments with sparse vegetation and adjacent high ground provide excellent conditions for good observation. Distance, light, and season must also be considered. Other factors that influence recognizability include the size and complexity of the target, the existence of distinctive target signatures, the presence of masking or camouflage, and the technical sophistication and training of the adversary.

A7.9.2. **Table A7.6 (Added-AMC)** shows how recognizability values are assigned on CARVER matrixes.

Table A7.6. Assigning Recognizability Values.

CRITERIA	SCALE
The target is clearly recognizable under all conditions and from a distance; it requires little or no training for recognition	9-10
The target is easily recognizable at small-arms range and requires a small amount of training for recognition	7-8
The target is difficult to recognize at night in bad weather, or might be confused with other targets or target component; it requires some training for recognition	5-6
The target is difficult to recognize at night or in bad weather, even with small-arms range; it is easily confused with other targets or components, it requires extensive training for recognition	3-4
The target cannot be recognized under any conditions, except by experts	1-2

A7.10. CARVER MATRIX

A7.10.1. These CARVER factors and their assigned values are used to construct a CARVER matrix. For the adversary this is a tool for rating the desirability of potential targets and wisely allocating attack resources. For the installation commander, it is a tool to counter the adversary.

A7.10.2. To construct the matrix, list the adversary's potential targets in the left column. For strategic level analysis, list the installations systems or subsystems (electric power supply, rail system). For tactical level analysis, list the complexes or components of the subsystems or complexes selected by your MEVA analysis. (**Table A9.7** shows a sample matrix for a bulk electric power supply facility.)

A7.10.3. As each potential target is evaluated for each CARVER factor, enter the appropriate targets have been evaluated, add the values for each potential target. The sums represent the relative desirability of each potential target; this constitutes a prioritized list of targets. Attack targets with the highest totals first.

A7.10.4. If additional men and/or munitions are available, allocate these resources to the remaining potential targets in descending numerical order. This allocation scheme will maximize the use of limited resources. Planners can use the CARVER matrix to present the installations staff with a variety of adversary defeat options. With the matrix they can discuss the strengths and weaknesses of each COA against the installations targeted facility.

Table A7.7. Complete CARVER Matrix.

An initial CARVER report and targeting folder that highlights gaps in the data may be prepared at this step. The folder is used to develop a detailed collection and reconnaissance and surveillance (R&S) plan For Example: THE INSTALLATION'S BULK ELECTRIC POWER SUPPLY							
POTENTIAL TARGETS	C	A	R	V	E	R	TOTAL
FUEL TANKS	8	9	3	8	5	6	41
FUEL PUMPS	8	6	2	10	5	3	34
BOILERS	6	2	10	4	5	4	31
TURBINES	8	6	10	7	5	9	45
GENERATORS	4	6	10	7	5	9	41
CONDENSERS	8	8	5	2	5	4	34
FEED PUMPS	3	8	5	8	5	4	33
CIR. WATER PUMPS	3	8	5	8	5	4	33
GENERATOR STEP UP TRANSFORMER	10	10	10	9	5	9	53

Attachment 8 (Added-DOVERAFB)

FORCE PROTECTION CONDITION VISUAL AIDS

Figure A8.1. AMCVA 10-245, Force Protection Condition ALPHA

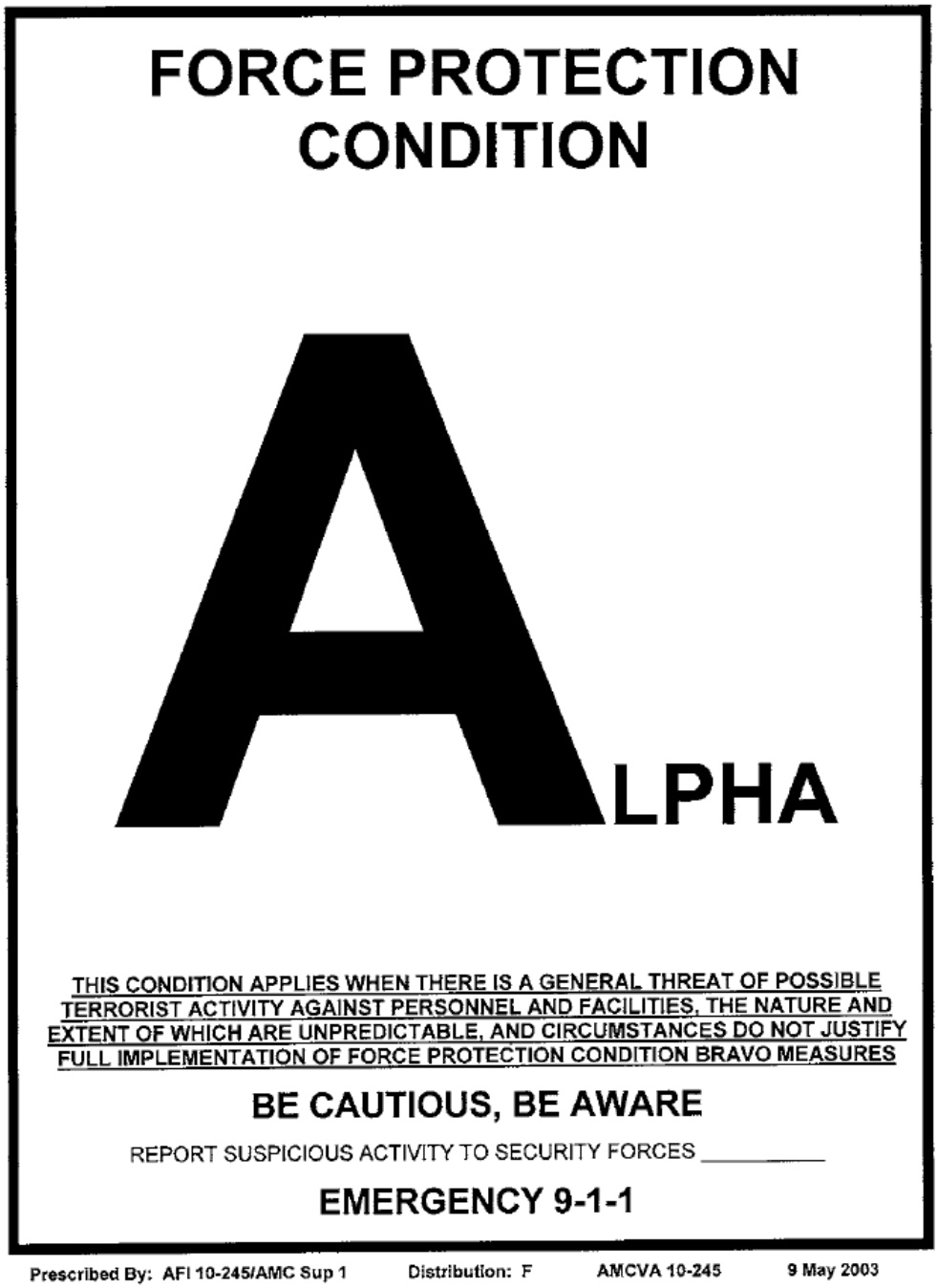


Figure A8.2. AMCVA 10-246, Force Protection Condition BRAVO

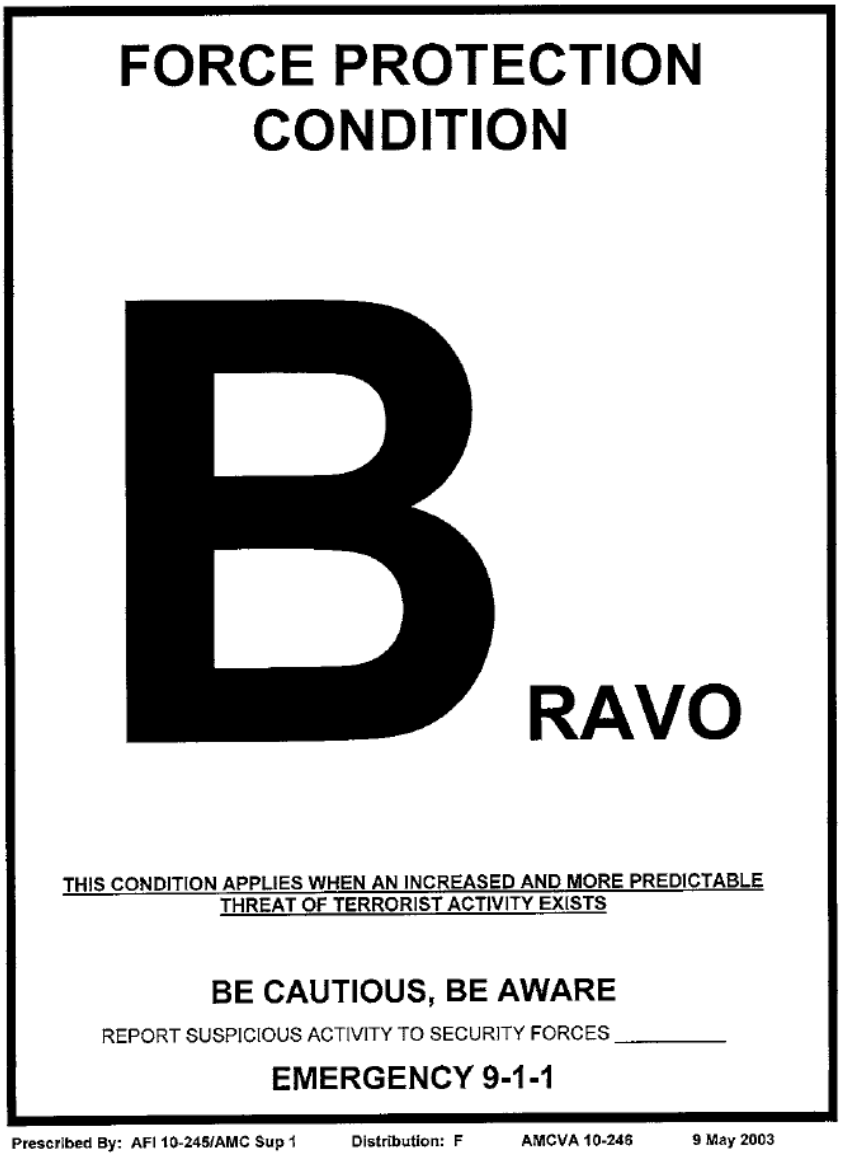


Figure A8.3. AMCVA, 10-247, Force Protection Condition CHARLIE

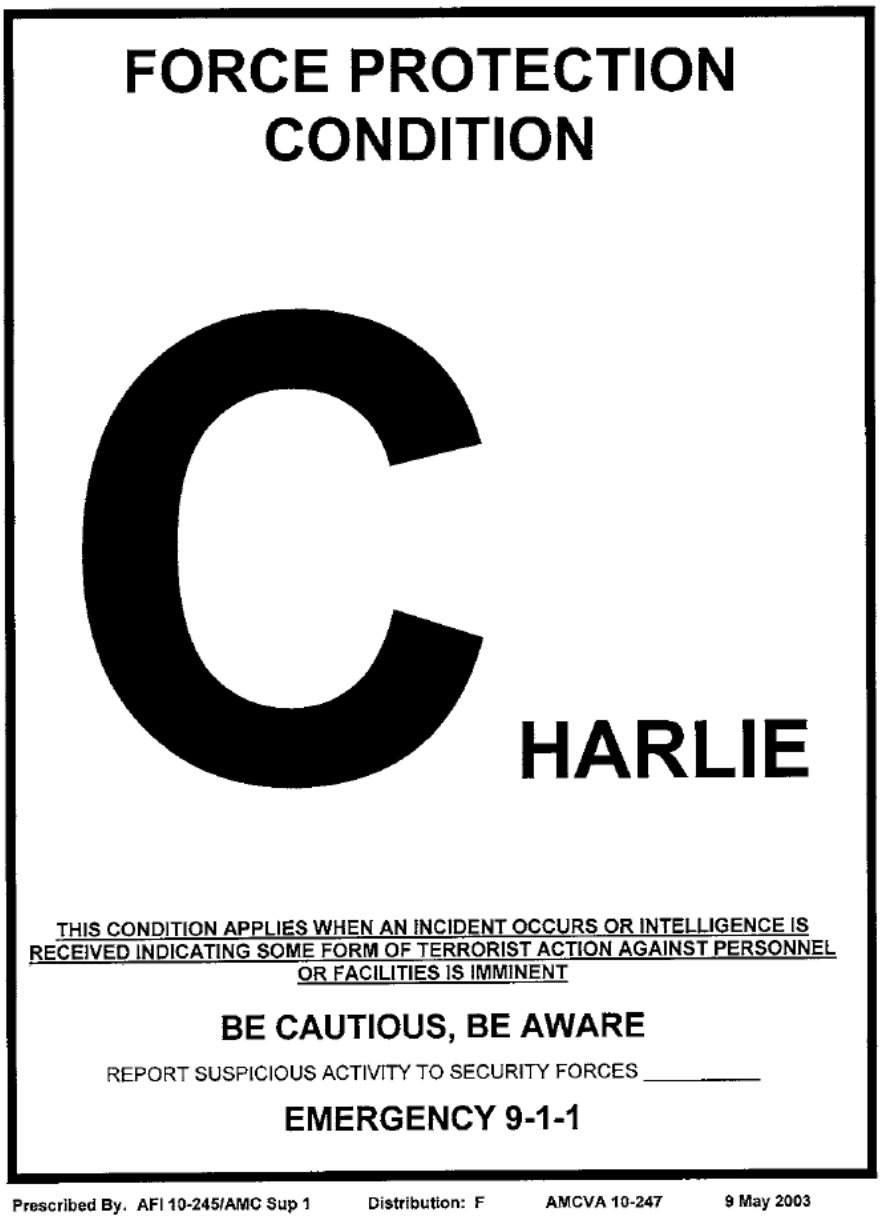
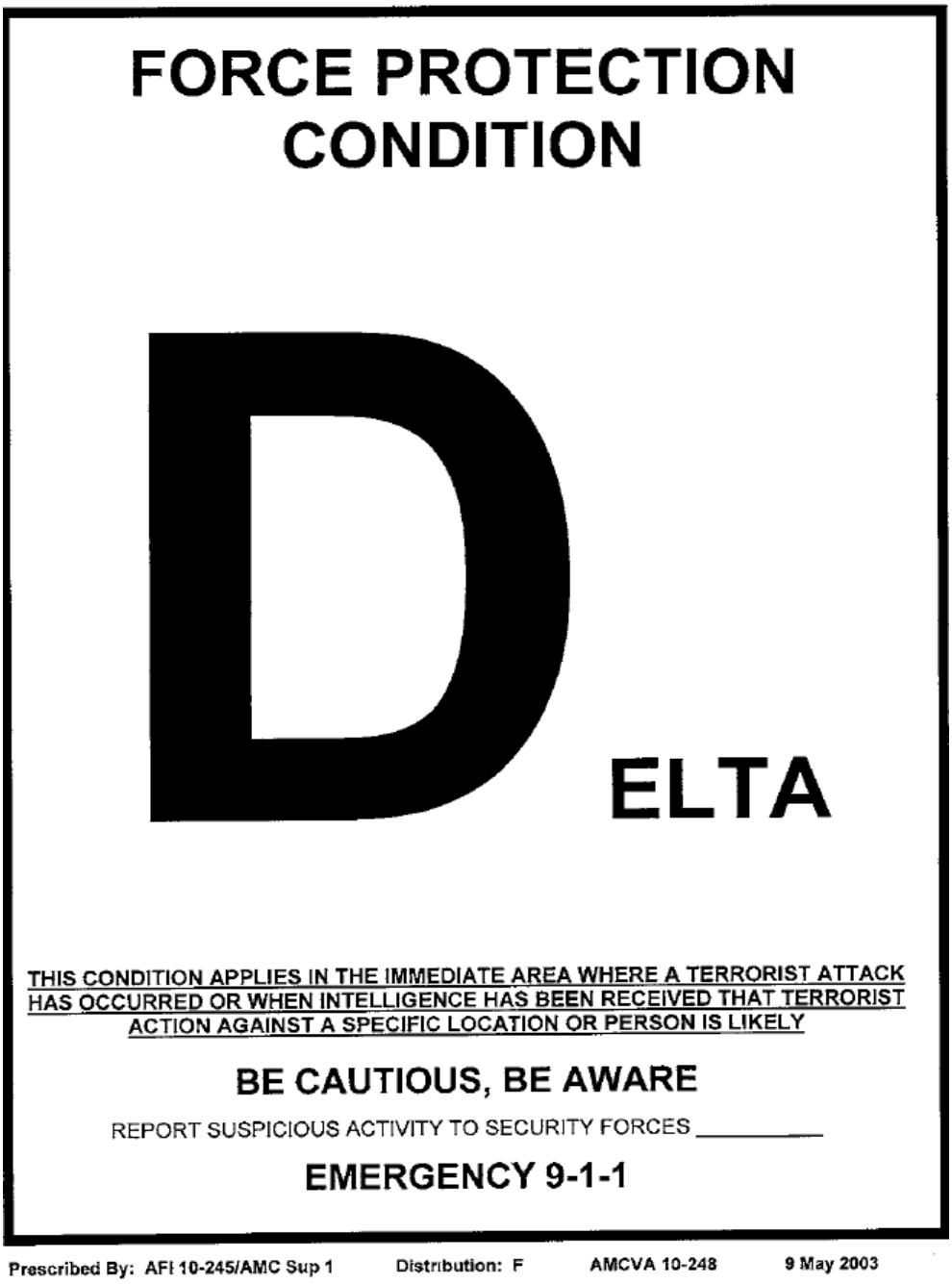


Figure A8.4. AMCVA 10-248, Force Protection Condition DELTA



Attachment 9 (Added-DOVERAFB)

SAMPLE LOCAL VA AND PROGRAM REVIEW LETTER

MEMORANDUM FOR: HQ AMC A7SA

SUBJECT: Annual Local Vulnerability Assessment and Local Program Review

FROM:

1. IAW AFI 10-245, AMC Sup 1, para 2.31.5.1, the (Wing) completed its annual local vulnerability assessment and local program review on DD Month Year. CVAMP will be populated with vulnerabilities discovered, along with corrective courses of action and mitigation measures, within 90 days from the date above. Also, the results from the program review will be entered into CVAMP within 30 days from the date above.

2. If you have any questions, please contact our POC, (Wing ATO) at DSN or email.

WING CC
Colonel, USAF

Commander

Attachment 10 (Added-DOVERAFB)

FORCE PROTECTION WORKING GROUP CHARTER

FORCE PROTECTION WORKING GROUP

CHARTER

MISSION:

The Force Protection Working Group (FPWG) is a cross-functional working group made up of Wing and tenant units. The FPWG serves as the primary advisory body to the Installation Commander on Antiterrorism (AT) and Force Protection (FP) policy, countermeasures and resource management in response to the assessed terrorist threat.

COMPOSITION OF ORGANIZATION:

The FPWG is Chaired by the Deputy Commander, 436th Mission Support Group (436 MSG/CD). Members of the FPWG are subject matter experts in their functional area and represent their respective commanders as decision-makers on AT/FP issues. Membership of the Dover FPWG includes:

Wing Antiterrorism Advisor (ATA)

AF Office of Special Investigations (AFOSI)

Communications (CS)

Civil Engineer (CE)

{Operations & Readiness}

Intelligence (IN)

Security Forces (SF)

Financial Management (FM)

Contracting Squadron (CONS)

Judge Advocate (JA)

Public Affairs (PA)

Force Support Squadron (FSS)

Wing Plans (XP)

Medical Group (MG)

{Public Health & Bioenvironmental}

Operations Group (OG)

Maintenance Group (MXG)

512th AT NCO (512 SFS)

Critical Infrastructure Protection (ATC)

Tenants and other agencies

PURPOSE OF ORGANIZATION:

The Force Protection Working Group (FPWG) forwards issues of concern affecting the Wing's force protection posture from all functional areas to the Force Protection Executive Council (FPEC). The FPWG addresses issues of concern, reaches possible courses of action (COAs) and presents recommendations and solutions to the Wing Commander through the FPEC.

The FPWG meets monthly or as directed by the Chair. Key responsibilities include:

1. Improve the overall force protection posture for the Installation

2. Coordinate and provide deliberate planning for all Antiterrorism/Force Protection issues
3. Analyze and track Installation vulnerabilities; coordinate mitigation measures
4. Reviews Installation vulnerabilities, prioritizes CVAMP entries, provide recommendations for resourcing decisions to mitigate identified vulnerabilities
5. Review FPCON measures semi-annually to ensure threat mitigation measures are appropriate
6. Conduct annual review of Installation Risk Assessments

Attachment 11 (Added-DOVERAFB)

THREAT WORKING GROUP CHARTER

THREAT WORKING GROUP

CHARTER

MISSION:

The Threat Working Group (TWG) serves as the principal advisory body to the Wing Commander for threat and intelligence reporting. The TWG is the focal point for intelligence information for Dover AFB whose primary responsibility is to address the criminal/terrorist threats and recommend courses of action (COAs) to mitigate or counter such threats.

COMPOSITION OF ORGANIZATION:

The TWG is a multi disciplinary fusion cell comprised of subject matter experts. The 436th Security Forces Commander has been designated as the Chair the TWG. The following are core TWG members: SF Operations, AT Advisor, AFOSI, IN and MDG (Public Health). Ad hoc members of the TWG consist of: 436 CS, 436 CES/CEX (Readiness), 436 CES/EOD, 436 MDG (Bioenvironmental), 512 AW/ATO and 512 AW/IN. The Wing Commander or TWG Chairman may add members from other agencies such as SV, PA, and JA (not all inclusive) as appropriate, to enhance the TWG or address specific threats or COAs. The TWG meets monthly or as directed by the Chair.

TWG members shall be dually accredited delegates of their organization and experts in their particular fields. Also, they shall also have a wide range of experience in recognizing attack indicators, detecting patterns of terrorist surveillance, targeting and planning, and have as a minimum, a working knowledge of Antiterrorism/Force Protection and counter-surveillance operations. AT Level II certification is highly recommended for all TWG members.

TWG members must fully understand the purpose of the TWG and be constantly proactive in seeking out information and intelligence from multiple sources (pull intelligence/info vs. waiting for a push). TWG members shall maintain open lines of communication with other Installation agencies in order to facilitate timely and accurate flow of threat information.

PURPOSE OF THE ORGANIZATION:

The TWG shall gather, analyze and promptly report any information or intelligence indicating a potential or actual threat to Dover AFB personnel or resources. The TWG will conduct risk analysis and develop COAs to counter or mitigate threats. The TWG will evaluate FPCON changes, RAMs, FPCON measures and forward recommendations to the Wing Commander and/or FPWG Chair.

POWERS OF ORGANIZATION:

The TWG shall have direct liaison authority with local, state and federal agencies required to

execute its mission. It will also have appropriate access to resources under the control of the Wing as deemed necessary by the 436 AW/CC, FPWG and/or TWG Chair's.

Unit	AT Officer or NCO Rank/Name	Date	FPCON Measure	Specific Action(s)/ Location(s)	Time Initiated	Time Terminated	Comments/ Remarks
436 AW/CP	Lt Smith	1 Jun 05	C.11.2	Searched all hand carried items of personnel entering the Cmd Post.	0001	0400	Wing Directed RAM
436 AW/CP	Lt Smith	1 Jun 05	B.1.0.3.1	Verified notification procedures, checklists, and rosters were current and valid for Installation Crisis Response/Consequence Management agencies and personnel	0823	0851	Functional Specific RAM
436 AW/CP	TSgt James	16 Jun 05	B.5.3	Consider closing all windows, blinds and curtains.	N/A	N/A	Wing Directed RAM--Not accomplished. Cmd Post only has one facility (Bldg 203) and has no windows.
436 AW/CP	Lt Smith	16 Jun 05	B.1.0.4	Posted person outside the CP to verify identity and proper open area on RAB of individuals entering CP.	1201	1600	Unit Specific RAM

Attachment 12 (Added-DOVERAFB)

AT FORM 2, RANDOM ANTITERRORISM MEASURE, TRACKING SHEET

INSTRUCTIONS

1. Review the monthly Wing RAM listing one week prior to the 1st of each month.
2. Ensure Wing-directed and organizational or functional specific RAMs are conducted.
3. Initiate/execute Wing-directed RAMs at the time indicated on the RAM listing.
4. Document all RAMs via AT Form 2, *RAM Tracking Sheet* upon completion.
5. In the event the RAM cannot be conducted at the directed time because personnel are not on duty, contact the AT office for a supplemental measure and date. ***Note:*** *Annotate the AT Form 2 with a detailed reason for non-compliance.*
6. Maintain AT Form 2, RAM Tracking Sheets in the Unit AT Continuity Book and forward a copy to the Wing AT office within 2 duty days of completing RAMs.

Attachment 13 (Added-DOVERAFB)

SAMPLE UNIT AT TRAINING REPORT

MEMORANDUM FOR 436 AW/AT

FROM: Unit/Agency

SUBJECT: Monthly Antiterrorism (AT) Training Report

1. In accordance with AFI 10-245, *The Air Force Antiterrorism (AT) Standards*, all active uniformed service members require annual Level I AT training. Furthermore, all DoD civilians will receive AT Level I training annually if the Terrorism Threat Level is above "MODERATE." AT Level I training shall also be offered to contract employees. Annual AT Level I Awareness training may be accomplished by any AT Level II certified personnel or by DoD sponsored computer-based training. Below are the AT Level I training statistics within the unit/agency :

AT Level I Training Stats	**Assigned:**	**Trained:**
Military	76	68
Civilian	19	19
Contractors	5	3
Total:	100	90

2. AT Level II training is required for installation level Antiterrorism Officers and personnel appointed to the Threat Working Group, Force Protection Working Group and Unit AT Representatives. The personnel listed below have successfully completed AT Level II training:

AT Level II Trained	**Date Trained**	**Last 4 SSN**	**Course Method**
MSgt John J. Smith	22 Mar 05	6789	CBT
SSgt William Tell	22 Mar 05	5673	In-residence

3. AT Level III training is designed for squadron and group commanders. The personnel listed below received AT Level III training:

AT Level III Trained	**Date Trained**	**Last 4 SSN**
Maj Neil Roberts	16 Feb 05	890-12-3456

4. Please direct any questions to MSgt Smith at 677-1234.

JOHN J. SMITH, MSgt, USAF
Unit Antiterrorism Representative

Attachment 14 (Added-DOVERAFB)

AT FORM 1, CVAMP TRACKING SHEET

Core Vulnerability Assessment Management Program (CVAMP) Tracking Sheet		
PROJECT TITLE: Install Screening Fence Around Emergency Generator		
CVAMP TRACKING #: T-AF-2005-0001		**PROJECT TRACKING (CES/CS) #:** 41020
OPR/UNIT OFFICE SYMBOL/DUTY PHONE: Capt Sample/436 SFS/SFOZ/X-6667		**ESTIMATED COST:** $30K
PROJECT DESCRIPTION: Install screening fence or wall and access gates around emergency generator at building 910 (SFS main facility).		
DATE	**FUNDED**	**STATUS/UPDATE**
1 Mar 05	No	SFS will coordinate with CES to evaluate the type of screening device and gate access points. CES will consider base appearance scheme when selecting construction materials. Cost estimates and type of screening system will be presented at the next FPWG meeting. CES indicated there is no funding available at this time. **ECD: Unknown (OPEN)**
1 Apr 05	Yes	CES received supplemental funding for AT/FP projects and can fund this project. Work is scheduled to begin 1 Jun 05 and should be complete by 31 Jul 05. The design of the gate is still being discussed. **ECD: 31 Jul 05 (OPEN)**
6 May 05	Yes	Project began as scheduled on 1 Jun 05 and there is no change to the estimated completion date. CES recommended the use of a steel gate. **ECD: 31 Jul 05 (OPEN)**
1 Jun 05	Yes	Wall construction completed. Gates are still on order and should be received by 1 Aug 05 pushing the ECD back two weeks. **ECD: 15 Aug 05 (OPEN)**
3 Jul 05	Yes	Gates were received early and installation was completed yesterday. **(Recommend Closure)**

Attachment 15 (Added-DOVERAFB)

436 AW/AT UNIT PROGRAM REVIEW GUIDE

(References: AFI 10-245, *Antiterrorism Program Standards*, AFI 10-245, AMC Supplement 1 and Dover AFB Supplement 1 unless otherwise noted)					
PR SCORE		**SUBJECT AREA**	**In Compliance**	**In Compliance with Comments**	**Not In Compliance**
	10 Points	**1. Continuity Book**			
	10	All required Sections and Content			
	8 Points	**2. Appointment of Unit AT Reps**			
	2	AT Appt Letter (Dated: _____)			
	2	Primary & Alt Designated/Current			
	1	Appointees E-5 or Above			
	2	Letter Signed by Unit Commander			
	1	Letter on File with AT Office			
	10 Points	**3. AT Level II Training**			
	2	Level II Training Current (within past 3yrs)			
	4	Primary & Alternate Reps Trained			
	2	CBT or In-Resident AT Level II within 60 Days of Appointment			
	2	AT Level II Training Certificates for AT Reps on file			
	10 Points	**4. RAM Schedule & AT Form 2**			
	2	AT Reps Understand the Wing RAM Program and Execution			
	2	Are Wing RAMs Conducted			
	2	Unit Specific RAMs Being			

		Conducted (Minimum: 1 per week)			
	2	. AT Form 2 Used to Record RAMs			
	2	. AT Form 2 Accurately Filled Out and Turned In Monthly (NLT 2nd of Month)			
PR SCORE		**SUBJECT AREA**	**In Compliance**	**In Compliance with Comments**	**Not In Compliance**
	8 Points	**5. AT Level I Training Statistics**			
	2	. Tracking System for AT Level 1-3 Training			
	4	. Wing AT Training Report Utilized and Turned in Monthly			
	2	. Unit Orderly Room Validates AT Level 1 during Web Leave Request Overseas			
	10 Points	**6. Self-Inspection Checklist/Results**			
	4	. Are Semi-annual Self-Inspections being conducted IAW Wing Policy			
	4	. Results of SI reported to Wing AT Office and endorsed by Unit CC			
	2	. Unit AT Program SI Checklist results maintained on file for 24 months			
	6 Points	**7. Wing FPCON Signs / Checklists**			
	2	Current FPCON Signs Displayed Properly on Access Points to all Facilities			
	2	. FPCON Signs for each level maintained on site for immediate use (i.e. Alpha, Bravo, Charlie and Delta)			
	2	Are Wing QRCs on-hand for all FPCONs			

	12 Points	**8. Unit FPCON Actions**			
	4	Unit Specific FPCONs Current			
	3	FPCON Checklists -- all assigned Buildings			
	3	Site Specific Barrier Plan on File & Current			
	2	If Applicable, are Expedient Barriers Available On Site for immediate Use			
	5 Points	**9. Shelter In-Place (SIP) Plan**			
	2	SIP Plan Current for the Bldg.			
	2	Shelter In-Place Location Identified			
	1	SIP Plan Exercised Annually			
PR SCORE		**SUBJECT AREA**	**In Compliance**	**In Compliance with Comments**	**Not In Compliance**
	6 Points	**10. Active Shooter (AS) Response**			
	3	Does the Unit have an AS Plan & Checklist			
	3	Are all personnel trained on AS response			
	10 Points	**11. Building Evacuation Plans**			
	3	Current Bomb Threat (BT) Evacuation Plan			
	2	Current Fire Evacuation Plan			
	2	Are Primary & Alternate Rally Points Established for each Plan			
	2	BT Evacuation Plan Exercised Annually			
	1	Identified Alarm for Bomb Threat			

	5 Points	12. AT Publications (Availability)			
	1	DoDI 2000-16, DoD AT Standards			
	1	DoD Handbook 2000-12-H			
	1	AFI 10-245, Antiterrorism Standards			
	1	AFI 10-245, AMC Sup 1 & Dover Sup 1			
	1	Wing AT OPlan 10-245 / Security OPlan 31-08			
TOTAL SCORE		OVERALL RATING			

0-50 Unsatisfactory	51-75 Marginal	76-84 Satisfactory	85-94 Excellent	95-100 Outstanding

EVALUATOR COMMENTS:

_____

_____

_____

Attachment 16 (Added-DOVERAFB)

SAMPLE UNIT AT REPRESENTATIVE APPOINTMENT LETTER

Date: _____

MEMORANDUM FOR 436 AW/AT

FROM: Unit/Agency

SUBJECT: Unit Antiterrorism Representative Appointment Letter

1. The following individuals are appointed as the Unit Antiterrorism Representatives for the 436th Example Squadron:

	Name	Clearance	AT Lvl II	D/P	Off/Sym
Primary:	TSgt John J. Smith	Secret	22 Feb 05	1234	SWROTS
Alternate:	SSgt Marc J. Brown	Secret	N/A	4321	SPQR

2. This letter supersedes previous letter, same subject.

JAMES T. SMITH, Major, USAF
Commander

cc: Each Individual

Attachment 17 (Added-DOVERAFB)

DOD CATEGORIES OF REPORTABLE SUSPICIOUS ACTIVITY

Reference: *DoD Instruction 2000.26, dated 1 Nov 11, Suspicious Activity Reporting*

1. ACQUISITION OF EXPERTISE. Unjustified attempts to obtain or conduct specialized training in security concepts, military weapons or tactics, or other unusual capabilities such as specialized transport or handling capabilities that would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

2. BREACH OR ATTEMPTED INTRUSION. Unauthorized entry or attempted entry into a restricted area or protected site; impersonation of authorized personnel (e.g., police, security, or janitorial personnel).

3. ELICITING INFORMATION. Suspicious questioning of personnel by any means about particular DoD structures, functions, personnel, or procedures at the facility or infrastructure.

4. EXPRESSED OR IMPLIED THREAT. A threat to DoD personnel or threatened damage to or compromise of a DoD facility or infrastructure.

5. FLYOVER OR LANDING. Suspicious overflight of or landing near a DoD facility or infrastructure by any type of flying vehicle (e.g., airplane, helicopter, unmanned aerial vehicle, hang glider).

6. MATERIALS ACQUISITION OR STORAGE. Acquisition of unusual quantities of precursor material (e.g., cell phones, pagers, fuel, and timers); unauthorized or unlicensed individual or group attempts to obtain precursor chemicals, agents, or toxic materials; or rental of storage units for the purpose of storing precursor material, chemicals, or apparatuses for mixing chemicals.

7. MISREPRESENTATION. Misusing or presenting false insignia, documents, or identification or engaging in any other activity to misrepresent one's affiliation.

8. RECRUITING. Building operations teams and developing contacts, or collecting personnel data, banking data, or travel data under circumstances that would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

9. SABOTAGE, TAMPERING, OR VANDALISM. Damaging, manipulating, or defacing part of a DoD facility, infrastructure, or protected site. Acts of vandalism committed by DoD civilian employees, military members, or their dependents should not be reported as suspicious activity unless those acts relate to a pattern of criminal activity or otherwise would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

10. SURVEILLANCE. Monitoring the activity of DoD personnel, facilities, processes, or systems, including showing unusual interest in a facility, infrastructure, or personnel (e.g., observation through binoculars, taking notes, drawing maps or diagrams of the facility, and taking pictures or video of a facility, infrastructure, personnel, or the surrounding environment) under circumstances that would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

11. TESTING OF SECURITY. A challenge to or a series of interactions with DoD installations, vessels, personnel, or systems that could reveal physical, personnel, or cyber security capabilities or vulnerabilities.

12. THEFT, LOSS, OR DIVERSION. Theft or loss associated with a DoD facility or infrastructure (e.g., of badges, uniforms, identification cards, emergency vehicles, technology, or documents, whether classified or unclassified) that are proprietary to the facility, or a diversion of attention from a DoD facility or infrastructure that is related to a theft or loss associated with that facility.

13. WEAPONS DISCOVERY. Discovery of weapons or explosives, as defined in section 930 of title 18, U.S.C. (Reference (n)). The discovery of personal weapons legally owned by DoD civilian employees, military members, or their dependents should not be reported as suspicious activity if the discovery is solely the result of the owner's failure to properly store or secure the weapon(s).

14. UNEXPLAINED ABSENCES OF INTERNATIONAL MILITARY STUDENTS. International military students who are unexpectedly absent from scheduled activities when the absence is without proper authorization and lasts more than 24 hours, and an appropriate official with the host DoD organization determines that the absence is not due to a misunderstanding in scheduling, due to sickness, or another similar reason

Attachment 18 (Added-DOVERAFB)

HOTEL ASSESSMENT SECURITY GUIDE

Evaluator: _____ Org: _____ Date: _____ Overall Score: _____

Facility Name: _____ POC Name: _____ Phone: _____

Section I – Security Design: (maximum of 10 points)		**C**	**P**	**N**
1.	HVAC; access control and emergency shut-off switch to mitigate TIC/TIM event?			
2.	Is there adequate vehicle stand-off from living quarters and mass gathering areas?			
3.	Is unobstructed space (10m from bldg) clear of overgrown shrubs, trees, vegetation?			
4.	Are barriers used to restrict access to service roads or enforce facility standoff?			
5.	Are loading areas controlled to prohibit parking of oversized vehicles next to bldg?			
Subtotal:				
Section II – Access Control: (maximum of 8 points)		**C**	**P**	**N**
1.	Is entry controlled/monitored to the facility? (i.e. doors, locks, alarms, etc)			
2.	Is access restricted to sensitive areas? (Comm /server room, HVAC systems, etc.)			
3.	Is storage of luggage locations restricted? (away from large gathering of people)			
4.	Is Single Point of Entry use during day-to-day operations?			
Subtotal:				

Section III – Physical Security Considerations: (maximum of 12 points)		**C**	**P**	**N**
1.	Does the facility have on-duty security personnel?			
2.	Is lighting adequate; (point/area) building, parking lot, interior/exterior?			
3.	Interior Lock for Occupant's Room (dead bolt or latch lock)			
4.	Are CCTV Cameras utilized on-site and are they operational? (Fixed, PTZ, etc.)			
5.	Are CCTV Cameras monitored real-time to detect approaching threats?			
6.	Do CCTV Cameras monitor all personnel entering/exiting the facility?			
Subtotal:				

Section IV – Employee Measures: (maximum of 6 points)		**C**	**P**	**N**
1.	***Are criminal background checks conducted on all employees? (critical item)***			
2.	Are employees released or fired for violent behavior reported to Law Enforcement?			
3.	Is there an active employee security awareness program?			
Subtotal:				

Section V – Threat Information: (maximum of 8 points)		**C**	**P**	**N**
1.	Is local Law Enforcement response time under 5 minutes?			
2.	Are external/internal threats reported to Law Enforcement for action?			
3.	Are suspicious activities reported immediately to local Law Enforcement?			
4.	Are active BOLOs posted or barred persons being tracked from the establishment?			

Subtotal:
LEGEND: Compliant or Yes = 2 pts Partial or Unknown = 1pt Non-Compliant or No = 0

HOTEL ASSESSMENT RISK ASSESSMENT MATRIX

NOTE: To be used in conjunction with the Hotel Assessment Security Guide **Risk Levels / Point Values**		**Risk Definitions**				
		Facility not recommended. No security features to protect DoD personnel.	***Facility not recommended for use by DoD personnel. Security is inadequate.***	***Facility is acceptable for limited use. Limited security features.***	***Facility is acceptable for use. Provides adequate security.***	***Facility is acceptable for use. Security program is robust.***
Critical	**0-10**					
High	**11-15**					
Medium	**16-21**					
Low	**21-35**					
Negligible	**36-44**					